Telindus 2400 series

Telindus 2400 series

User and reference manual

Version: 1.3 - 191771

Telindus Technical Publications – Geldenaaksebaan 335 - B-3001 Leuven - Belgium – Tel. +32 16 382011

Document properties

Subject	Telindus 2400
Manual type	User and reference manual
Version	1.3
Code	191771
Modification date	22 July 2004 ©Telindus

Copyright notice

The information and descriptions contained in this publication are the property of Telindus. Such information and descriptions must not be copied or reproduced by any means, or disseminated or distributed without the express prior written permission of Telindus.

This publication could include technical inaccuracies or typographical errors, for which Telindus never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new editions of this publication. Telindus may make improvements and/or changes in the product(s) described in this publication at any time, without prior notice.

Safety requirements

Carefully read the safety instructions at the beginning of 2 - Installing and connecting the Telindus 2400 on page 19.

The connectors of the Telindus 2400 should only be connected to the following circuit types:

Connector name	Connector label	Connector type	Circuit type
control connector	CTRL	subD-9	SELV
G703 station clock connector	CLK	RJ45	SELV
alarm connectors	ALM IN/OUT	RJ45	SELV
LAN connector	LAN	RJ45	SELV
SHDSL lines connector	LINES	TELCO-50	TNV-1
modular interface connector	(none)	(depends on the type of interface)	SELV

- SELV (Safety Extra Low Voltage): local connection (e.g. PC to Telindus 2400) or leased line inside the building.
- TNV-1 (Telecom Network Voltage): leased line outside the building.
- TNV-2: PSTN from PABX inside the building.
- TNV-3: PSTN from operator PABX outside the building.

Statements

CE

www.telindusproducts.com → Telindus Access Solutions → Products → Choose a product → Downloads → Certificates

Hereby, Telindus declares that this Telindus 2400 complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Hierbij verklaart Telindus dat deze Telindus 2400 overeenstemt met de essentiële vereisten en andere relevante bepalingen van Richtlijn 1999/5/EC.

Par la présente, Telindus déclare que ce Telindus 2400 est en conformité avec les exigences essentielles et autres articles applicables de la Directive 1999/5/EC.

Hiermit, Telindus erklärt daß dieser Telindus 2400 in Fügsamkeit ist mit den wesentlichen Anforderungen und anderen relevanten Bereitstellungen von Direktive 1999/5/EC.

Mediante la presente, Telindus declara que el Telindus 2400 cumple con los requisitos esenciales y las demás prescripciones relevantes de la Directiva 1999/5/CE.

A Telindus declara que o Telindus 2400 cumpre os principais requisitos e outras disposições da Directiva 1999/5/EC.

Col presente, Telindus dichiara che questo Telindus 2400 è in acquiescenza coi requisiti essenziali e stipulazioni attinenti ed altre di Direttivo 1999/5/EC.

Με το παρον, η Telindus δηλωνει οτι το Telindus 2400 ειναι συμμορφουμενο με τις βασικες απαιτησεις και με τις υπολοιπες σχετικες διαταξεις της οδηγιας 1999/5/EC.

The Telindus 2400 documentation set

The documentation set of the Telindus 2400 currently consists of the following:

Document	Description
Telindus 2400 manual (this manual)	This is the manual you are reading now. It shows you how to install and connect the Telindus 2400 and gives you a basic configuration. It also contains a complete description of all the configuration, status, performance and alarm parameters for look-up purposes.
maintenance and management application manuals	The Telindus 2400 can be maintained and managed by a variety of maintenance and management tools. Refer to 1.6 - Maintenance and management tools on page 15 for an introduction on these tools and for a reference to the manual of these tools.
cable documents	A wide variety of cables exist to connect the Telindus 2400. The Data cables document (PDF) and the Management cables document (PDF) describe these cables.

All these documents, together with the free maintenance tool TMA and the firmware of the Telindus devices, can be found on the Telindus Access Products distribution CD that is delivered with all Telindus products.

Organisation of this manual

This manual contains the following main parts:

Part	This part …
User manual	shows you how to install and connect the Telindus 2400. It also gives a basic configuration of the Telindus 2400.
Reference manual	gives more detailed information on the Telindus 2400, such as software download procedures, technical specifications, etc. It also contains a complete description of all the configuration, status, performance and alarm parameters for look-up purposes.
Annex	gives additional information, such as product sales codes.

Refer to the Table of contents on page ix for a detailed overview of this manual.

Typographical conventions

The following typographical conventions are used in this manual:

The format …	indicates …
Normal	normal text.
Italic	• new or emphasised words • application windows, buttons and fields. E.g. In the *File name* field enter …
`Computer`	text you have to enter at the DOS or CLI prompt, computer output and code examples. E.g. `NOK,1,1,Invalid command.`

`Computer Bold`	text you have to enter at the DOS or CLI prompt when it is part of a mix of computer input and output.
	E.g.
	`/o1003:"Edit Configuration"`
	`>`**`get sysName`**
	`  sysName = "Orchid 1003 LAN"`
	`/o1003:"Edit Configuration"`
	`>`

Narrow	containment tree objects and attributes of a device when they are mentioned in the normal text. I.e. when they are not a part of computer input or output. E.g. Use the sysName attribute in order to …
<Narrow>	containment tree objects or attributes or part of them that are variable. I.e. depending on the product version, used interface, etc. the names of these objects or attributes are slightly different. E.g. topObject/<modularIf>/someAttribute means that the name of the object <modularIf> depends on which modular interface you use. For example, v35 in case of a V.35 interface, g703 in case of a G.703 interface, etc.
Blue	references to other parts in the manual. E.g. “Refer to xx - Title for more information”.
Blue underline	• a hyperlink to a web site. E.g. www.telindus.com • a reference to another manual. E.g. “Refer to the TMA manual (PDF) for more information”. The abbreviation between brackets is an indication of the file format (PDF = Portable Document Format / CHM = Compiled HTML Help).

Graphical conventions

The following icons are used in this manual:

Icon	Name	This icon indicates …
	Remark	remarks or useful tips.
	Caution	text to be read carefully in order to avoid damage to the device.
	Warning	text to be read carefully in order to avoid injury.
	DIP switch	a DIP switch or strap table.
	Basic attribute	a basic attribute in the containment tree of the Telindus 2400.
	Advanced attribute	an advanced attribute in the containment tree of the Telindus 2400.
	Structured attribute	a structured attribute within another attribute in the containment tree of the Telindus 2400.
	Action	an action in the containment tree of the Telindus 2400.

Reading a DIP switch table

At several places in this manual DIP switch tables are shown. To enable you to read such a table in a correct manner it is explained below.

A DIP switch table has the following layout:

DIP switch name	DS1 no.	Setting	Funtion
	1	**on**	
		off	

1 2 3 4 5

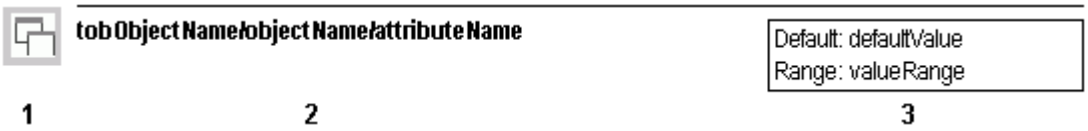
The following table explains the DIP switch configuration table layout:

Number	This position displays …
1	the DIP switch icon.
2	the DIP switch name.
3	the DIP switch position on the DIP switch bank. The abbreviations mean the following: DS1 no. 1: DIP switch bank number 1, switch position number 1
4	the possible settings of the DIP switch: on and off. The default setting is printed in bold.
5	the function associated with the corresponding DIP switch setting.

Reading an attribute string

At several places in this manual attribute strings are shown. To enable you to read such a string in a correct manner it is explained below.

An attribute string has the following layout:



1 2 3

The following table explains the attribute string layout:

Number	This position displays …
1	the attribute icon. It indicates that the string which follows is an attribute string. Refer to Graphical conventions on page vi for more information.
2	the attribute name and its position in the containment tree.
3	the default value of a configuration attribute.

Application software version

This manual describes the features, containment tree and attributes of the Telindus 2400 application software version …

- T2402/00300 (Telindus 2400 SHDSL models).
- T2403/00300 (Telindus 2400 ADSL Annex A models).
- T2404/00300 (Telindus 2400 ADSL Annex B models).

Audience

This manual is intended for computer-literate people, who have a working knowledge of computing and networking principles.

Your feedback

Your satisfaction about this purchase is an extremely important priority to all of us at Telindus. Accordingly, all electronic, functional and cosmetic aspects of this new unit have been carefully and thoroughly tested and inspected. If any fault is found with this unit or should you have any other quality-related comment concerning this delivery, please submit the Quality Comment Form on our web page at www.telindusproducts.com/quality.

Table of contents

User manual 1

1 Introducing the Telindus 2400 3
1.1 What is the Telindus 2400? 4
1.2 Functional diagram of the Telindus 2400 5
1.3 Simplified protocol diagram of the Telindus 2400 6
1.4 Telindus 2400 series overview 9
1.5 Telindus interface modules (TIMs) overview 14
1.6 Maintenance and management tools 15
1.7 Maintenance and management tools connection possibilities 17

2 Installing and connecting the Telindus 2400 19
2.1 Safety instructions 20
2.2 Unpacking 21
2.3 Installation and connection precautions 22
2.4 Installing the Telindus 2400 as table top 23
2.5 Installing the Telindus 2400 as rack mount 24
2.6 Connecting the Telindus 2400 25
2.7 The front panel LED indicators 33

3 DIP switches of the Telindus 2400 37
3.1 The Telindus 2400 motherboard 38
3.2 DIP switches of the Telindus 2400 39
3.3 Opening and closing the housing 40

4 Maintaining the Telindus 2400 41
4.1 Maintaining the Telindus 2400 with TMA 42
4.2 Introducing the management terminology 48
4.3 The objects in the Telindus 2400 containment tree 52
4.4 Adding an object to the containment tree 56
4.5 Telindus 2400 attribute overview 61

5 Configuring the Telindus 2400 - the concept of profiles 63
5.1 Explaining profiles 64
5.2 How to create a configuration using profiles? 74

6 Basic configuration 85
6.1 What is an interface? 86
6.2 Configuring IP addresses 87
6.3 Configuring the SHDSL line 97
6.4 Configuring the ADSL line 104
6.5 Configuring passwords 107
6.6 Executing configuration actions 110
6.7 Troubleshooting the Telindus 2400 114

7 Configuring the encapsulation on the xDSL lines 115
7.1 Configuring ATM encapsulation 116
7.2 Configuring PPP encapsulation (in case of PPPoA) 137

8 Configuring the encapsulation on the TIMs 153
8.1 Configuring IMA on the 6E1 interface 154
8.2 Configuring ATM on the E3/T3 interface 159

9 Configuring routing 165
9.1 Introducing routing 166
9.2 Enabling routing on an interface 167
9.3 Configuring static routing 168
9.4 Configuring policy based routing 176
9.5 Configuring the Routing Information Protocol 182
9.6 Configuring address translation 191
9.7 Configuring traffic and priority policy on the router 207

10 Configuring bridging 223
10.1 Introducing bridging 224
10.2 Configuring bridging 234
10.3 Configuring traffic and priority policy on the bridge 245

11 Configuring switching 249
11.1 Introducing switching 250
11.2 Configuring VLAN switching 251
11.3 Configuring ATM switching 256

12 Configuring the additional features 265
12.1 Configuring DHCP 266
12.2 Configuring an extended access list 271
12.3 Configuring VLANs 278
12.4 Configuring L2TP tunnels 282
12.5 Configuring IP security 289

Reference manual 295

13 Configuration attributes 297
13.1 Configuration attribute overview 298
13.2 General configuration attributes 306
13.3 LAN interface configuration attributes 312
13.4 Cascading configuration attributes 320
13.5 4 port Ethernet interface configuration attributes 322
13.6 6E1 interface configuration attributes 323
13.7 E3/T3 interface configuration attributes 333
13.8 IMA group configuration attributes 349
13.9 xDSL interface configuration attributes 352
13.10 Profile configuration attributes 354
13.11 ATM switching configuration attributes 398
13.12 Router configuration attributes 400
13.13 Bridge configuration attributes 445
13.14 Alarm in contacts configuration attributes 456
13.15 SNMP configuration attributes 459
13.16 Management configuration attributes 461
13.17 Loopback configuration attributes 470

14 Status attributes 473
14.1 Status attribute overview 474
14.2 General status attributes 481
14.3 LAN interface status attributes 486
14.4 Cascading status attributes 494
14.5 4 port Ethernet interface status attributes 496
14.6 6E1 interface status attributes 497
14.7 E3/T3 interface status attributes 502
14.8 IMA group status attributes 509
14.9 xDSL interface status attributes 515
14.10 ATM status attributes 535
14.11 Profile status attributes 542
14.12 Router status attributes 544
14.13 Bridge group status attributes 562
14.14 Management status attributes 569
14.15 Loopback status attributes 571
14.16 File system status attributes 573
14.17 Operating system status attributes 576

15 Performance attributes 579
15.1 Performance attributes overview 580
15.2 LAN interface performance attributes 585
15.3 4 port Ethernet interface performance attributes 589
15.4 6E1 interface performance attributes 590
15.5 E3/T3 interface performance attributes 595
15.6 IMA group performance attributes 601
15.7 xDSL interface performance attributes 603
15.8 ATM performance attributes 613
15.9 Router performance attributes 617
15.10 Bridge performance attributes 629
15.11 Management performance attributes 634
15.12 Operating system performance attributes 637

16 Alarm attributes 641
16.1 Alarm attributes overview 642
16.2 Introducing the alarm attributes 645
16.3 General alarms 649
16.4 LAN interface alarms 651
16.5 4 port Ethernet interface alarms 652
16.6 6E1 interface alarms 653
16.7 E3/T3 interface alarms 654
16.8 xDSL interface alarms 655
16.9 Router alarms 662
16.10 Alarm in contacts alarms 663

17 TMA sub-system picture 665

18 Auto installing the Telindus 2400 667
18.1 Automatically obtaining an IP address using BootP or DHCP 668
18.2 Automatically obtaining an IP address on the LAN 669
18.3 Obtaining the configuration with TFTP 670
18.4 Creating configuration files 673
18.5 Creating a binary configuration file 674
18.6 Creating an ASCII configuration file 675

19 Downloading software 679
19.1 What is boot, loader and application software? 680
19.2 Downloading application software 682
19.3 Downloading loader software 688
19.4 Downloading files to the file system 690

20 Technical specifications 691
20.1 Telindus 2400 models 692
20.2 Power requirements 693
20.3 Control connector specifications 694
20.4 Station clock connector specifications 695
20.5 Alarm in connector specifications 696
20.6 Alarm out connector specifications 697
20.7 xDSL line specifications 698
20.8 LAN interface specifications 703
20.9 TIM interface specifications 704
20.10 ATM encapsulation specifications 707
20.11 PPP encapsulation specifications 707
20.12 Frame Relay encapsulation specifications 707
20.13 IP routing specifications 709
20.14 Bridging specifications 709
20.15 Routing and bridging performance specifications 709
20.16 ATM switching performance specifications 709
20.17 Maintenance and management support 710
20.18 Memory specifications 710
20.19 Dimensions 710
20.20 Safety compliance 711
20.21 Over-voltage and over-current protection compliance 711
20.22 EMC compliance 711
20.23 Environmental compliance 711

Annex 713

Annex A:common TCP and UDP numbers 715

Annex B:product information 717

Index 721

User manual

1 Introducing the Telindus 2400

This chapter gives an introduction to the Telindus 2400. The following gives an overview of this chapter:

- 1.1 - What is the Telindus 2400? on page 4
- 1.2 - Functional diagram of the Telindus 2400 on page 5
- 1.3 - Simplified protocol diagram of the Telindus 2400 on page 6
- 1.4 - Telindus 2400 series overview on page 9
- 1.5 - Telindus interface modules (TIMs) overview on page 14
- 1.6 - Maintenance and management tools on page 15
- 1.7 - Maintenance and management tools connection possibilities on page 17

1.1 What is the Telindus 2400?

The Telindus 2400 access concentrator enables service providers to deploy business services over ADSL or SHDSL, while maintaining a maximum flexibility for the connection to the backbone.

Apart from a fixed 10/100Base-T backbone connection, the Telindus 2400 access concentrator can accept various modular interfaces with support for various encapsulation protocols. These Telindus interface modules (TIMs) include: 4 port 10/100Base-T Ethernet, 6E1, E3/T3 and STM1.

The Telindus 2400 supports full IP-routing, bridging, ATM switching and VLAN switching. In addition is has an extended support for IP CoS (Class of Service) and it can initiate and terminate VPN (Virtual Private Network) circuits. Therefore, the Telindus 2400 access concentrator can be used for supporting services like VoIP (Voice over IP) and intranet applications.

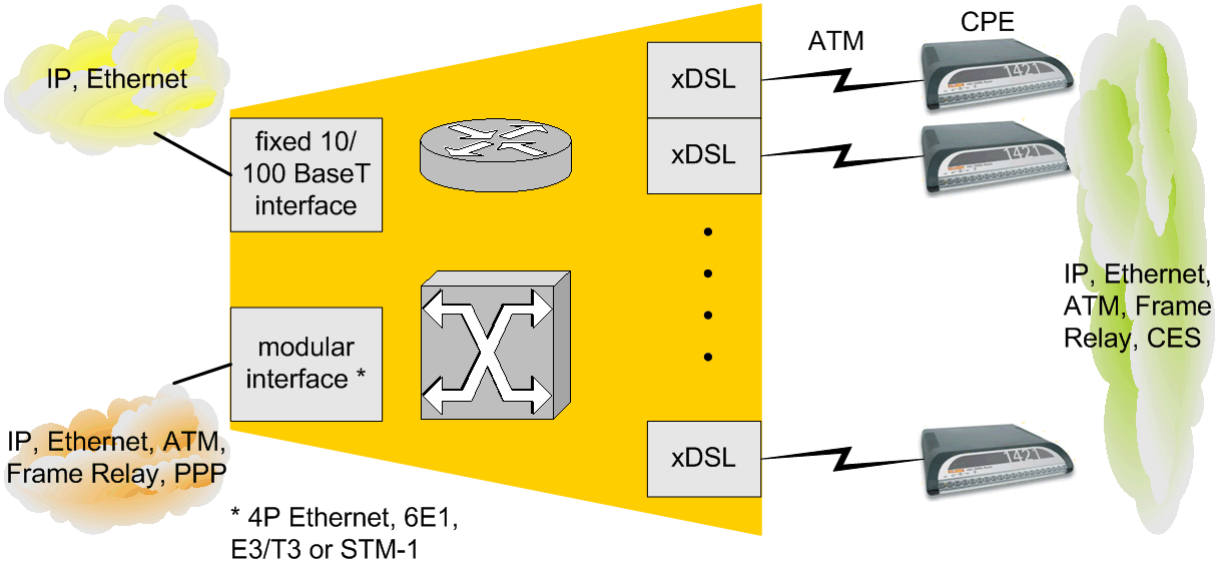
The Telindus 2400 access concentrator houses 8, 16 or 24 ADSL or SHDSL modems and multiple units can be cascaded through the 100Base-T Ethernet interface. In case of the Telindus 2400 SHDSL model, two SHDSL circuits can also be combined to increase the distance or speed towards the end-users. The equipment can be used as desktop equipment or can be rack-mounted (19” or ETSI).

The unit comes with a built-in management agent, so no additional hardware for network management is needed. The unit can be controlled locally by means of a craft terminal or can be managed remotely over IP. In this way the existing IP infrastructure can be used to transport all management information to a central location without the need for a separate overlay network.

Typical applications include the roll-out of business-oriented services over DSL as it is applicable in operator or campus network environments.

1.2 Functional diagram of the Telindus 2400

By using the appropriate CPE at the end-user site, the Telindus 2400 access concentrator can provide IP, VLAN, ATM, Frame Relay and CES services based on SHDSL or ADSL transmission technology.



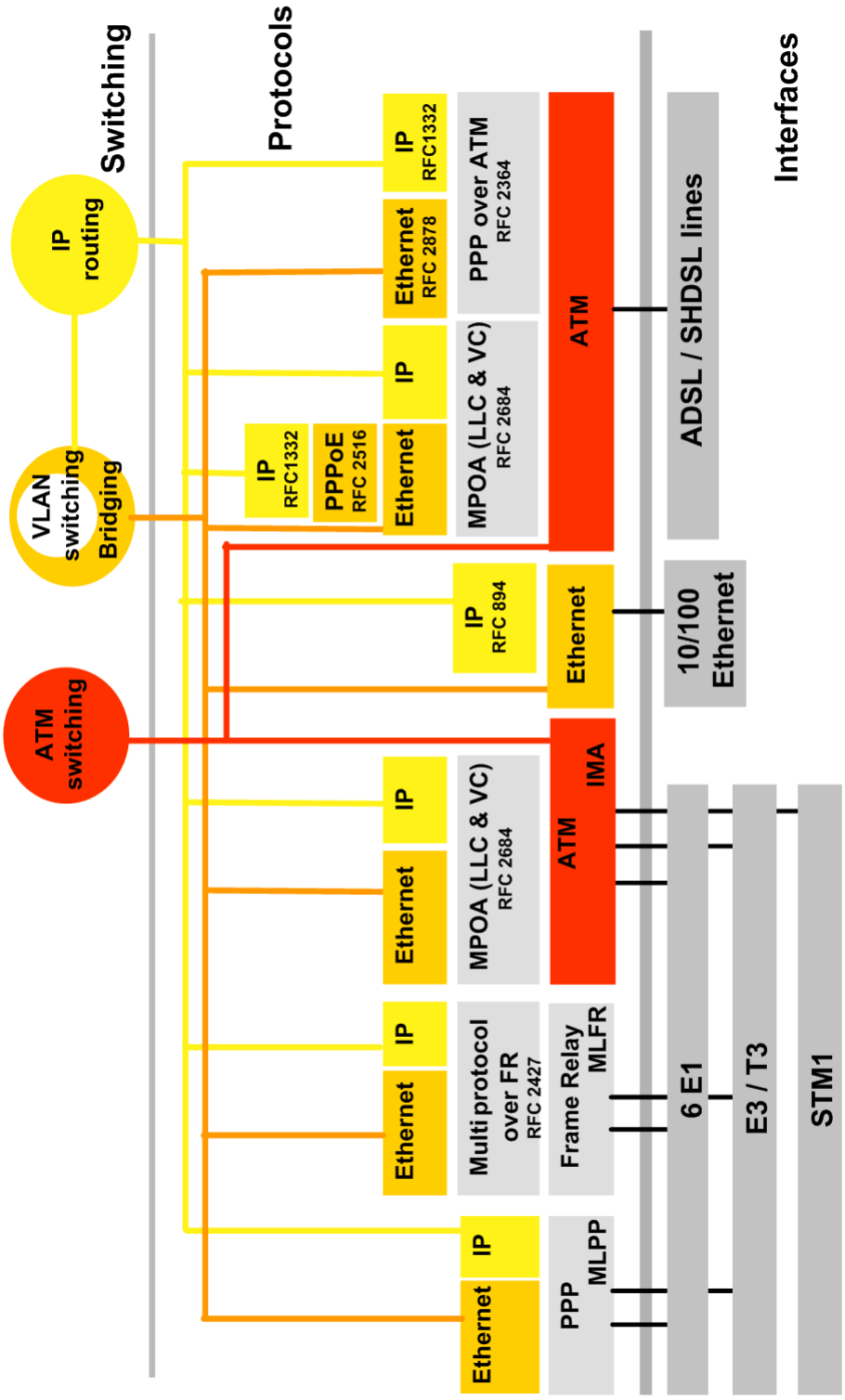
1.3 Simplified protocol diagram of the Telindus 2400

This section displays and describes the simplified protocol diagram of the Telindus 2400. The following gives an overview of this section:

- 1.3.1 - What shows the simplified protocol diagram? on page 7
- 1.3.2 - How to read the simplified protocol diagram? on page 8

1.3.1 What shows the simplified protocol diagram?

Below you can find a simplified protocol diagram of the Telindus 2400. The simplified protocol diagram shows in one figure the Telindus 2400 its physical interfaces, the protocols that are supported on these interfaces and the possible switching modes.



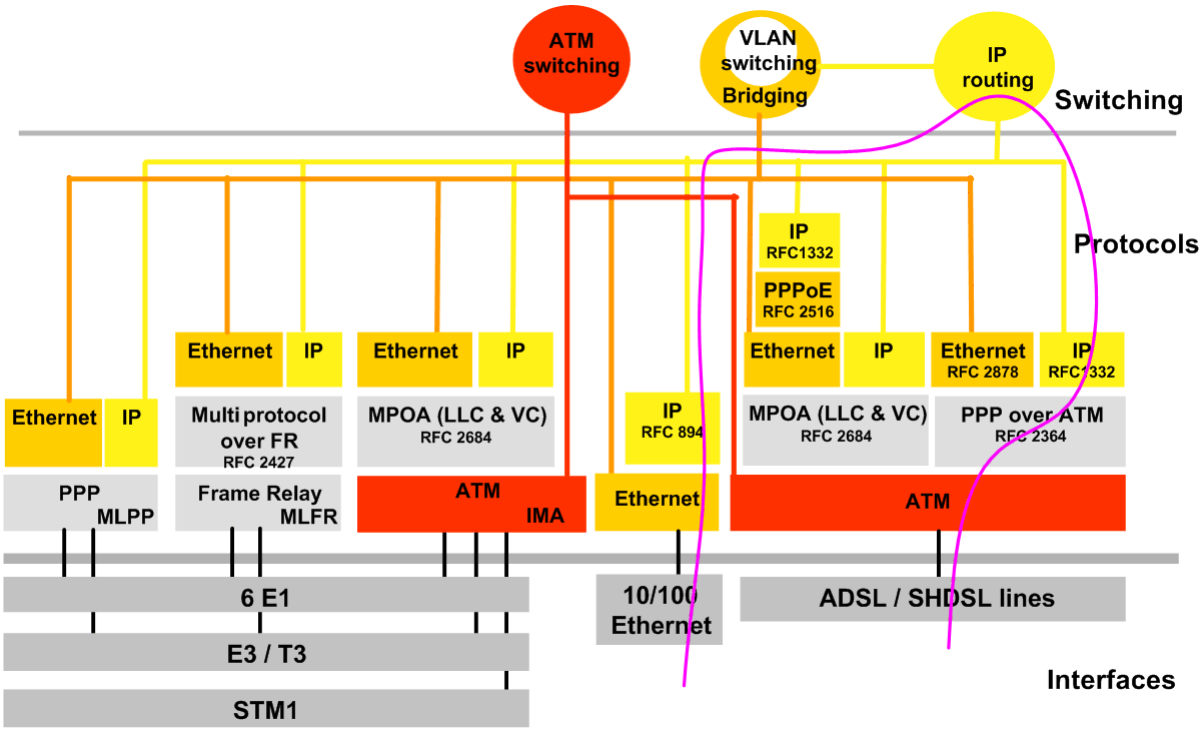
1.3.2 How to read the simplified protocol diagram?

The lines between the physical interface blocks, the protocol blocks and the switching blocks represent the path the data can follow when it goes through the Telindus 2400.

Example:

Suppose you connect a remote site using a CPE (e.g. a Telindus 1421 SHDSL Router) over an SHDSL line with the Telindus 2400. The used protocols on the SHDSL line are, in ascending layer order, ATM, PPP over ATM and IP. Then your data is routed to a backbone which is, for example, reachable through the fixed Ethernet interface. The used protocols on the Ethernet interface are, in descending layer order, IP and Ethernet.

If you map this on the simplified protocol diagram of the Telindus 2400, you get the following:



1.4 Telindus 2400 series overview

The Telindus 2400 series is a range of access concentrator each with their own specific features. This section gives an overview of all the members of the Telindus 2400 series.

The following gives an overview of this section:

- 1.4.1 - Telindus 2400 models on page 10
- 1.4.2 - Telindus 2400 front panels on page 11
- 1.4.3 - How to determine which Telindus 2400 model you have? on page 12

1.4.1 Telindus 2400 models

The Telindus 2400 series consists of the following models and sub-models:

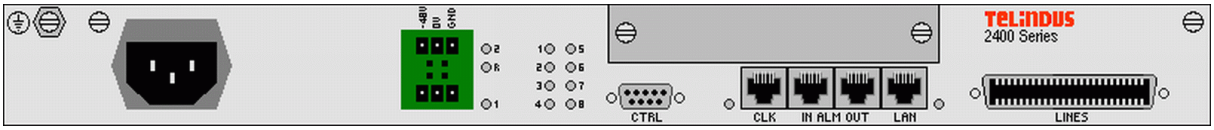
		Number of lines		
		8	16	24
ADSL lines	Annex A (ATM only)	**Telindus 2401** Sub-models: • -48 Vdc, with POTS splitter • -48 Vdc, without POTS splitter • -48 Vdc/Vac, with POTS splitter • -48 Vdc/Vac, without POTS splitter	**Telindus 2402** -48 Vdc and without POTS splitter only.	**Telindus 2403** -48 Vdc and without POTS splitter only.
	Annex B (ATM only)	**Telindus 2401** Sub-models: • -48 Vdc, with POTS splitter • -48 Vdc, without POTS splitter • -48 Vdc/Vac, with POTS splitter • -48 Vdc/Vac, without POTS splitter	**Telindus 2402** -48 Vdc and without POTS splitter only.	**Telindus 2403** -48 Vdc and without POTS splitter only.
SHDSL lines	ATM	**Telindus 2421** Sub-models: • -48 Vdc • -48 Vdc/Vac	**Telindus 2422** -48 Vdc only	**Telindus 2423** -48 Vdc only

1.4.2 Telindus 2400 front panels

This section displays the different front panels that exist for the Telindus 2400 series.

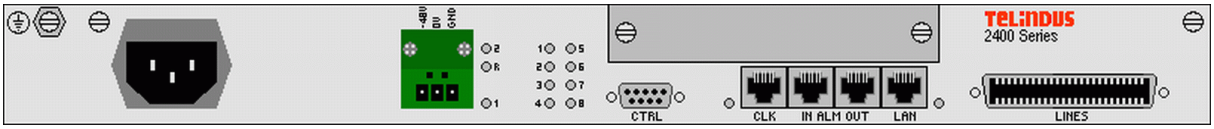
Telindus 2401 and 2421, -48 Vdc

The following shows the front panel of the Telindus 2401 and 2421 with a -48 Vdc power connector only.



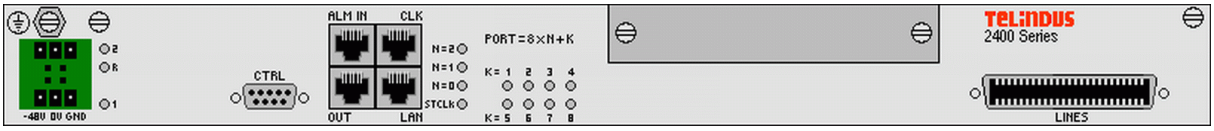
Telindus 2401 and 2421, -48 Vdc and 115/230 Vac

The following shows the front panel of the Telindus 2401 and 2421 with a -48 Vdc and a 115/230 Vac power connector.



Telindus 2402, 2403, 2422 and 2423

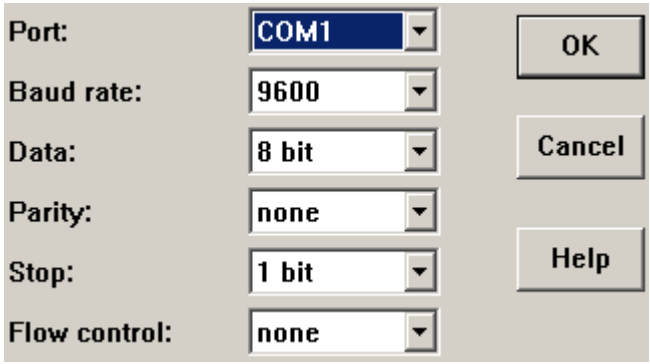
The following shows the front panel of the Telindus 2402, 2403, 2422 and 2423.



1.4.3 How to determine which Telindus 2400 model you have?

Because it is no longer possible to determine exactly which Telindus 2400 model you have by looking at the physical features of the device, you have to do it by connecting to the device.

The following procedure describes a simple way to check which Telindus 2400 model you have:

Step	Action
1	Connect the power supply to the Telindus 2400. Depending on your model, connect the -48 Vdc or 115/230 Vac. Refer to 2.6 - Connecting the Telindus 2400 on page 25.
2	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 2400.
3	Open a terminal emulation program on your computer (e.g. Tera Term). Make sure the connection parameters of the terminal emulation program are set as specified in 20.3 - Control connector specifications on page 694. 
4	Start a terminal session on the Telindus 2400 and press the *Enter* key. ⇒The string `Password:` appears in the terminal window.

5	By default no password is present. Therefore, just press the *Enter* key.
	⇒The following appears in the terminal window:
	`Login successful -- CLI active -- connecting with device`
	`>`
	`/telindus24xx:"Edit Configuration"`
	`>`

Step	Action

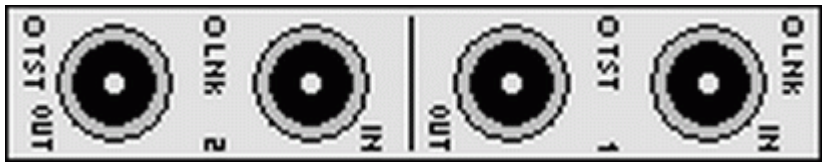
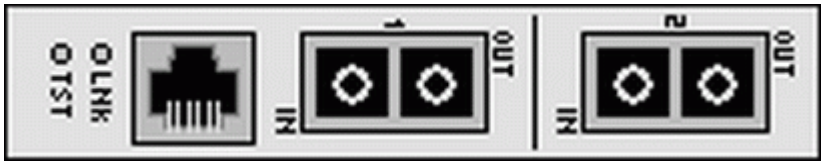
6	Type `selgrp Status`. By doing this you swap from the configuration parameters to the status parameters.
	⇒The following appears in the terminal window:
	`>selgrp Status`
	`OK`
	`/telindus24xx:Status`
	`>`

7	Type `get`. This retrieves the general status attributes of the Telindus 2400.
	⇒The following appears in the terminal window:
	`>get`
	`sysDescr = "Telindus 2401 ADSL Annex B T24xx/00100 01/01/04 12:00"`
	`sysObjectID = 1.3.6.1.4.1.776.63`
	`sysUpTime = "0d 0h 52m 37s"`
	`sysServices = 4`
	`flash1Version = "T24xx/00100 01/01/04 12:00"`
	`flash2Version = "T24xx/00100 01/01/04 12:00"`
	`activeFlash = flash2`
	`flashVersions = 2`
	`...`

8	The text after the sysDescr parameter displays which Telindus 2400 model you have. ⇒For example: `sysDescr = "Telindus 2401 ADSL Annex B"`

1.5 Telindus interface modules (TIMs) overview

Apart from a fixed 10/100Base-T backbone connection, the Telindus 2400 can accept various Telindus interface modules (TIMs). The following table gives an overview:

TIM	Short description
4 port Ethernet	Encapsulations: IEEE 802.3 (10 Mbps Ethernet) and IEEE 802.3u (100 Mbps Ethernet).
6E1	Supported layer 2 protocols: ATM IMA.
E3/T3	Supported layer 2 protocols: ATM. The E3/T3 interface exists in two versions: • a single E3/T3 version: • a dual E3/T3 version: 
STM1	Supported layer 2 protocols: ATM. 

1.6 Maintenance and management tools

The Telindus 2400 is manageable in many different ways. This section gives a quick overview of the various maintenance and management tools.

Maintenance or management tool	Description and reference
TMA	TMA (Telindus Maintenance Application) is a free Windows software package with a comprehensive graphical user interface that enables you to control the Telindus products completely. I.e. to access their configuration attributes and look at status, performance and alarm information. Refer to 4 - Maintaining the Telindus 2400 on page 41 and the TMA manual (PDF) for more information.
TMA Element Management	TMA Element Management is a management application designed to monitor large numbers of Telindus devices. It combines the easy to use graphical interface of the stand-alone version of TMA with an event-logging application called the Element Viewer. Refer to the TMA Element Management manual (PDF/CHM) for more information.
TMA for HP OpenView	TMA for HP OpenView is the management application that runs on the widely spread network management platform HP OpenView. It combines the easy to use graphical interface of the stand-alone version of TMA with the advantages and features of HP OpenView. Refer to the TMA for HP OpenView manual (PDF) for more information.
TMA CLI	TMA CLI (TMA Command Line Interface) enables you to use its commands in scripts in order to automate management actions. This is particularly useful in large networks. TMA CLI is a complementary product to TMA, TMA Element Management and TMA for HP OpenView. Refer to the TMA CLI manual (PDF) for more information.
ATWIN	ATWIN is a menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic, textual representation using a VT100 terminal. Refer to the Maintenance tools manual (PDF) for more information.
CLI	CLI is also a Command Line Interface, although not so extensive as TMA CLI. Experienced users who are familiar with the syntax can access the Telindus devices more quickly than with TMA or ATWIN. Refer to the Maintenance tools manual (PDF) for more information.
Web Interface	The Web Interface is an ATWIN alike menu-driven user interface. You can read and change all attributes as with TMA, but in a more basic representation using a web browser. Refer to the Maintenance tools manual (PDF) for more information.
EasyConnect terminal	Connecting the Telindus EasyConnect hand-held terminal through the control connector to the Telindus 2400, allows you to manage the Telindus 2400 in a basic way using the LCD display and keyboard. This is called keyboard management. Refer to the EasyConnect manual (PDF) for more information.

Maintenance or management tool	Description and reference
SNMP	You can manage the Telindus 2400 through SNMP using any SNMP browser. The Telindus 2400 supports MIB2 and a private MIB, including traps. The private MIB comes with your copy of TMA. After installation of the TMA data files, the private MIB file is available in directory *C:\Program Files\TMA\snmp*[1] with the name *<filename>.mib*[2]. Refer to 13.15 - SNMP configuration attributes on page 459 and the documentation of your SNMP browser for more information.

1. The first part of the directory path may be different if you did not choose the default path during the installation of the TMA data files.
2. The filename is product dependent. To determine which MIB file corresponds with which product, refer to the *models.nms* file (located in *C:\Program Files\TMA\model*[1]).

1.7 Maintenance and management tools connection possibilities

The following table gives an overview of all the maintenance and management tools and how you can connect them with the Telindus 2400:

Maintenance or management tool	Tool - Telindus 2400 connection		Tool - management concentrator connection[1]	
	Serial[2]	IP[3]	Serial[2]	IP[3]
EasyConnect	X		X	
CLI	X[4]	X[5]	X[4]	X[5]
ATWIN	X[4]	X[5]	X[4]	X[5]
TMA	X	X	X	X
TMA CLI	X	X	X	X
TMA Element Management		X		X
TMA for HP OpenView		X		X
SNMP[6]		X		X
Web Interface[7]		X		X

1. Examples of management concentrators are the Orchid 1003 LAN, the Telindus 1030 Router series, the Telindus 2300 SHDSL series, etc. Refer to their corresponding manuals for more information on how to set these devices up as management proxy.
2. A serial connection is a connection between the COM port of your PC and the control connector of the Telindus 2400 using a male-female DB9 cable.
3. An IP connection is a connection between your PC and the Telindus 2400 over an IP network.
4. Using a VT100 terminal (emulation program).
5. Using Telnet.
6. Using an SNMP browser.
7. Using a web browser.

2 Installing and connecting the Telindus 2400

First this chapter gives some important safety instructions. Then it explains how to install and connect the Telindus 2400.

You are advised to read this chapter from the beginning to the end, without skipping any part. By doing so, your Telindus 2400 will be completely installed and ready for configuration when you reach the end of this chapter.

The following gives an overview of this chapter:

- 2.1 - Safety instructions on page 20
- 2.2 - Unpacking on page 21
- 2.3 - Installation and connection precautions on page 22
- 2.4 - Installing the Telindus 2400 as table top on page 23
- 2.5 - Installing the Telindus 2400 as rack mount on page 24
- 2.6 - Connecting the Telindus 2400 on page 25
- 2.7 - The front panel LED indicators on page 33

2.1 Safety instructions

IMPORTANT SAFETY INSTRUCTIONS

Disconnect the power supply before installing, adjusting or servicing the unit.

Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

When installing the unit, the ground connection must always be made first and disconnected last.

ACHTUNG! WICHTIGE SICHERHEITSINSTRUKTIONEN

Vor sämtlichen Arbeiten am Gerät (Installation, Einstellungen, Reparaturen etc.) sollten Sie die Stromzufuhr unterbrechen.

Auf keinen Fall den Erdungsleiter unwirksam machen oder das Gerät ohne einen sachgerecht installierten Erdungsleiter verwenden. Wenn Sie sich nicht sicher sind, ob eine sachgerechte Erdung vorhanden ist, wenden Sie sich an den zuständigen elektrischen Fachmann oder einen Elektriker.

Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.

SAFETY WARNING

To avoid damage to the unit, please observe all procedures described in this chapter.

SICHERHEITSBESTIMMUNGEN

Um eine Beschädigung des Gerätes zu verhindern, beachten Sie bitte unbedingt die Sicherheitsbestimmungen die in diesem Abschnitt beschrieben werden.

Ensure that the unit and its connected equipment all use the same power and ground, to reduce noise interference and possible safety hazards caused by differences in ground or earth potentials.

2.2 Unpacking

Checking the shipping carton

Rough handling during shipping causes most early failures. Before installation, check the shipping carton for signs of damage:

- If the shipping carton is damaged, please place a claim with the carrier company immediately.
- If the shipping carton is undamaged, do not dispose of it in case you need to store the unit or ship it in the future.

Package contents

The box should contain the following items:

- Telindus 2400 (depending which model you ordered this is a Telindus 2401, 2402, 2403, 2421 or 2422, 2423).
- Self-adhesive plastic feet.
- TMA CD-ROM (including this User and Reference manual in PDF format).

2.3 Installation and connection precautions

ESD WARNING

The circuit boards are sensitive to electrostatic discharges (ESD) and should be handled with care. It is advisable to ensure an optimal electrical contact between yourself, the working area and a safety ground before touching any circuit board. Take special care not to touch any component or connector on the circuit board.

EMC WARNING

EMC compliant installation

The Telindus access products are fully EMC compliant. To ensure compliance with EMC directive 89/336/EEC, shielded cables or ferrite beads have to be used.

NOTE

This unit may be powered by an IT power system.

2.4 Installing the Telindus 2400 as table top

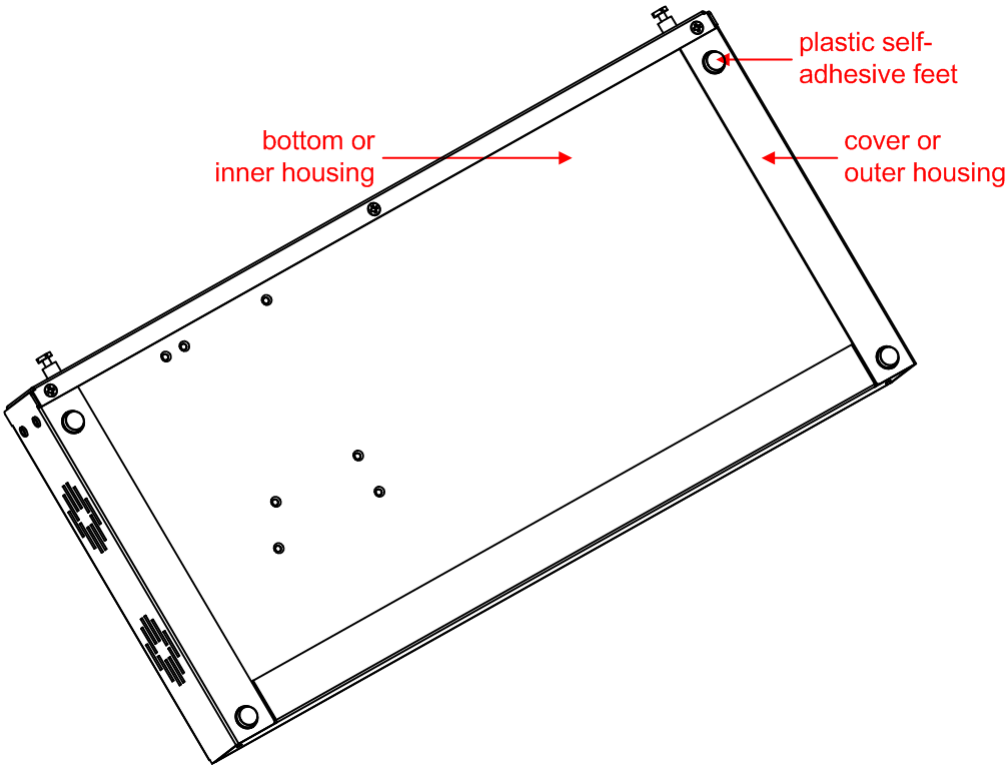
You can install the Telindus 2400 …

- as table top, i.e. as stand-alone version.
- as rack mount, i.e. mounted in a 19” or ETSI rack.

If you want to install the Telindus 2400 as table top, proceed as follows:

Step	Action
1	Take the Telindus 2400 out of the shipping carton.
2	Place the Telindus 2400 on a table in front of you with the bottom side up.
3	Take the self-adhesive plastic feet out of the box and paste them in the corners of the outer housing as shown in the figure below.
4	Turn the Telindus 2400 around again (top side up) and place it in a suitable location. When installing the Telindus 2400, consider the following: • Always place the unit on its feet. • Do not block the air vents. • Install the unit in an area free of extreme temperatures, humidity, shock and vibration. • Position the unit so that you can easily access the front panel with its connectors. • Leave enough clearance at the front for cables and wires. • Position the unit in the vicinity of the different connection points (power outlet, etc.).

Pasting the self-adhesive plastic feet on the Telindus 2400



2.5 Installing the Telindus 2400 as rack mount

You can install the Telindus 2400 …

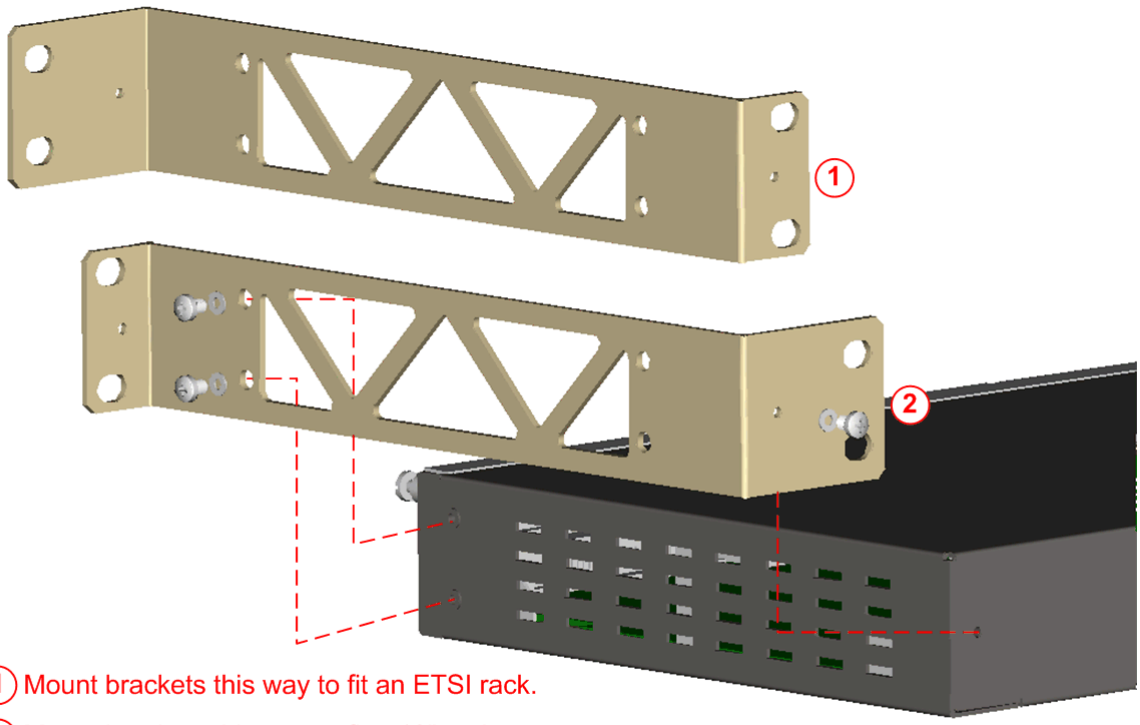
- as table top, i.e. as stand-alone version.
- as rack mount, i.e. mounted in a 19” or ETSI rack.

The rack mount brackets and screws are *not* included! They have to be ordered separately.

If you want to install the Telindus 2400 as rack mount, proceed as follows:

Step	Action
1	Take the Telindus 2400 out of the shipping carton.
2	Take the rack mount brackets and screws and mount them on the Telindus 2400 as shown in the figure below. Note that when you want to mount the Telindus 2400 in a ETSI rack you have to mount the rack mount brackets differently than when you want to mount it in an 19” rack!
3	Mount the Telindus 2400 in your 19” or ETSI rack.

Mounting the rack mount brackets and screws on the Telindus 2400



1 Mount brackets this way to fit an ETSI rack.

2 Mount brackets this way to fit a 19" rack.

Mount brackets both on right and left side of the device.

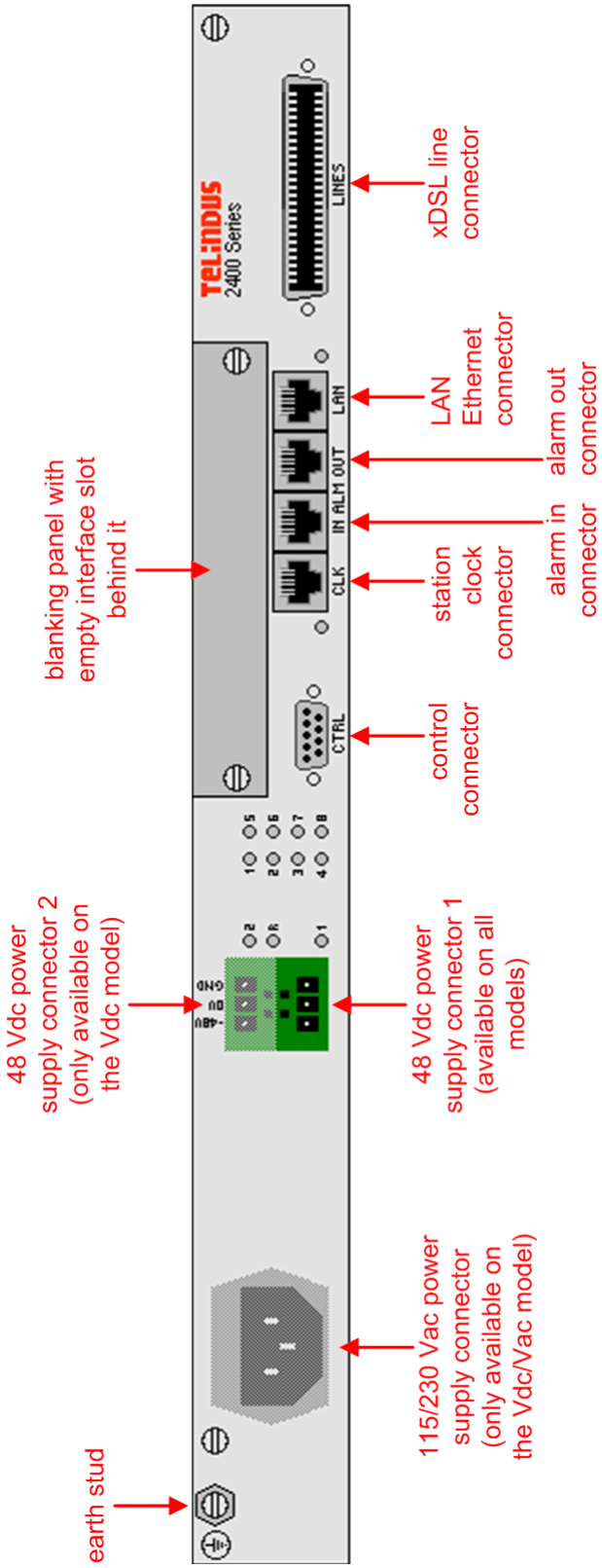
2.6 Connecting the Telindus 2400

This section explains how to connect the Telindus 2400. The following gives an overview of this section:

- 2.6.1 - Front view of the Telindus 2400 on page 26
- 2.6.2 - Connecting the different parts of the Telindus 2400 on page 27

2.6.1 Front view of the Telindus 2400

The following figure gives a front view of the Telindus 2401/2421:



Refer to 2.6.2 - Connecting the different parts of the Telindus 2400 on page 27 for a short description of each connector.

2.6.2 Connecting the different parts of the Telindus 2400

All connections have to be made at the front of the Telindus 2400 (refer to 2.6.1 - Front view of the Telindus 2400 on page 26).

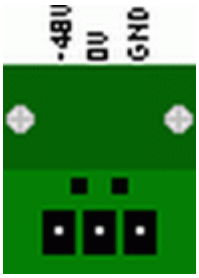
When you connect the cables to the different connectors of the Telindus 2400, make sure that you fasten each connector to the front panel by means of its screws or other locking mechanism. This in order to avoid that the cables get disconnected should you accidently pull at them.

The following table gives an overview of the connectors and reveals their function:

Connector label	Function
	This is the earth stud. For safety reasons, connect the earth wire to this stud. When installing the unit, the ground connection must always be made first and disconnected last. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
<no label> 	This connector is only present on the Vdc/Vac model. Refer to 1.4 - Telindus 2400 series overview on page 9. This is the 115/230 Vac power input. The selection between 115 Vac or 230 Vac is made automatically. You can connect a 115/230 Vac power supply to this connector and a -48 Vdc power supply to the -48 Vdc connector for power back-up purposes. Refer to 20.2 - Power requirements on page 693 for the power specifications of the Telindus 2400.

<table>
<tr><th>Connector label</th><th>Function</th></tr>
<tr><td>-48V
0V
GND</td><td>

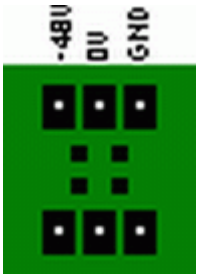
The single -48 Vdc power connector



This connector is only present on the Vdc/Vac model. Refer to 1.4 - Telindus 2400 series overview on page 9.

This is the -48 Vdc power input. You can connect a -48 Vdc power supply to this connector and a 115/230 Vac power supply to the 115/230 Vac connector for power back-up purposes.

The dual -48 Vdc power connector



This connector is only present on the Vdc model. Refer to 1.4 - Telindus 2400 series overview on page 9.

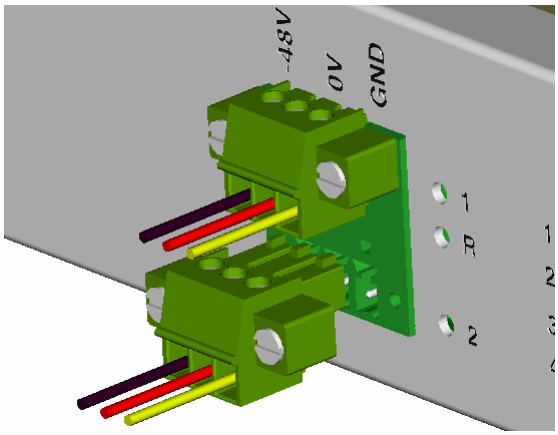
This is the -48 Vdc power input. You can connect two separate -48 Vdc power supplies for power back-up purposes.

Connecting the -48 Vdc power supply

The -48 Vdc power supply plug(s) is/are already plugged in the -48 Vdc power supply socket(s). You have to wire the -48 Vdc power supply plug(s) first:

Step	Action
1	Unscrew the two screws of the power supply plug.
2	Pull the power supply plug out of the power supply socket.
3	Connect the -48 Vdc, 0 Vdc and the protective ground to the plug as indicated on the front panel (-48V / 0V / GND).
4	Plug the power supply plug in the power supply socket.
5	Fasten the two screws of the power supply plug.

The following figure shows the procedure above:



Refer to 20.2 - Power requirements on page 693 for the power specifications of the Telindus 2400.

</td></tr>
</table>

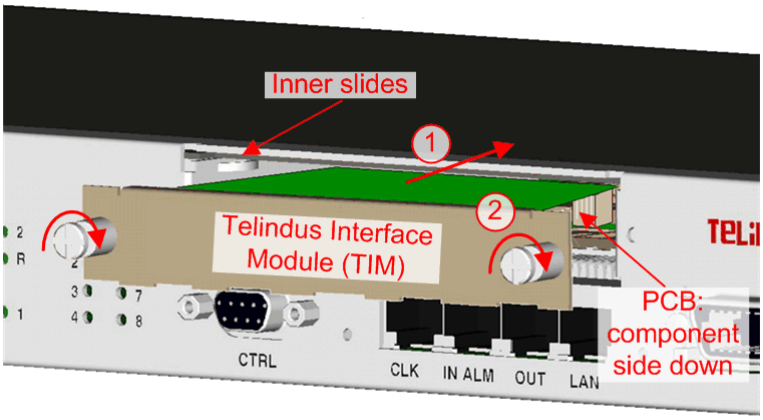
Connector label	Function
CTRL	This female 9-pins subD connector is the control connector. You can connect this connector to a COM port of your PC with a straight male-female DB9 cable (not included). This enables you to manage the Telindus 2400 locally, using TMA, CLI, ATWIN etc. Refer to … • 4.1 - Maintaining the Telindus 2400 with TMA on page 42 for more information on how to connect with TMA through the control connector. • 20.3 - Control connector specifications on page 694 for the control connector lay-out.
CLK	This RJ45 connector is the station clock connector. If you want to use station clocking, then connect the station clock to this connector. Refer to … • telindus24xx/hexE1/ifClocking on page 325 for more information on clocking. • 20.4 - Station clock connector specifications on page 695 for the station clock connector lay-out.
ALARM IN	This RJ45 connector is an alarm in connector. Using this connector you can generate an internal alarm (in the Telindus 2400) in case an external alarm condition occurs. For example, using the alarm in connector and a contact you could generate an internal alarm in case the door of the 19” or ETSI rack is open. Because the alarm is generated in the Telindus 2400, you can also send it to the central management station. Refer to … • 13.14 - Alarm in contacts configuration attributes on page 456 for more information on using the alarm in contacts. • 16.2.1 - Alarm configuration attributes on page 646 for more information on alarms in general. • 20.5 - Alarm in connector specifications on page 696 for the alarm in connector lay-out.
ALARM OUT	This RJ45 connector is an alarm out connector. Using this connector and its high and low alarm contacts, you can generate an external alarm in case an internal alarm condition occurs (in the Telindus 2400). For example, using the alarm out connector and contacts you could generate an external alarm (e.g. a buzzer that goes off) in case one of the xDSL lines goes down. Refer to … • 16.2.1 - Alarm configuration attributes on page 646 for more information on alarms and alarm contacts. • 20.6 - Alarm out connector specifications on page 697 for the alarm out connector lay-out.

Connector label	Function
LAN	This RJ45 connector is the LAN connector. Connect one side of an RJ45 to RJ45 cable (not included) to the LAN connector of the Telindus 2400 and the other side to an Ethernet network outlet. If you want to connect the Telindus 2400 to … • a regular Ethernet network outlet, then use a crossed RJ45 cable. • an Ethernet hub, then use a straight RJ45 cable. Refer to … • 13.3 - LAN interface configuration attributes on page 312 for more information on how to configure the LAN interface. • 20.8 - LAN interface specifications on page 703 for the LAN connector lay-out.
LINES	This 50-pins TELCO connector is the ADSL/SHDSL line connector. Connect the connector on one side of the TELCO cable (not included) to the xDSL line connector. Connect the wires at the other side of the TELCO cable to an xDSL outlet. **Important remarks** • For optimum performance, only use a *properly* twisted TELCO 25*2*CAT5 cable. Make sure that *even inside the connector assembly* the line pairs are properly twisted! The TELCO 25*2*CAT5 cable can be ordered separately. To find the relevant sales codes, refer to the Data cables document (PDF) on the Telindus Access Products distribution CD that was delivered with the Telindus 2400. • The Telindus 24x1 models are available with and without internal POTS splitter. Note that the line connector lay-out is not the same in both cases. Refer to … • 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to set up a connection. • 20.7.3 - xDSL line connector specifications on page 701 for the line connector lay-out without a POTS splitter. • and 20.7.4 - ADSL line connector specifications with POTS splitter on page 702 for the line connector lay-out with a POTS splitter (Telindus 24x1 models with internal POTS splitter only).

<table>
<tr><th>Connector label</th><th>Function</th></tr>
<tr><td><no label>
 </td><td>This is the blanking panel. Behind it is an empty interface slot. Use this interface slot to insert an optional Telindus interface module (TIM). Refer to 1.5 - Telindus interface modules (TIMs) overview on page 14.

To insert an interface module in the Telindus 2400, proceed as follows:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Loosen the two screws of the blanking panel and remove the blanking panel.</td></tr>
<tr><td>2</td><td>Take the interface module and turn it in such a way that the component side (i.e. the side on which the connectors are mounted) of the PCB faces down.</td></tr>
<tr><td>3</td><td>Gently slide the interface module on the two inner slides into the Telindus 2400.</td></tr>
<tr><td>4</td><td>Fasten the screws of the interface module.</td></tr>
</table>

(1) Slide the interface module in the empty slot.
(2) Fasten the screws of the interface module.</td></tr>
</table>

2.7 The front panel LED indicators

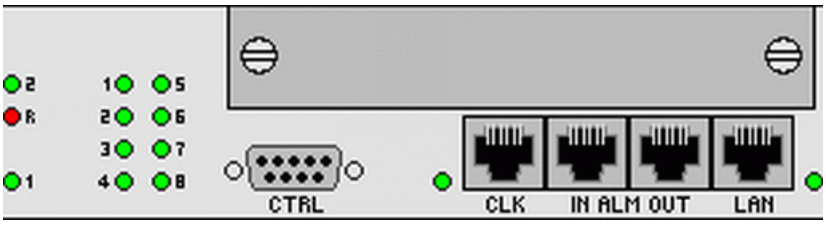
This section gives an overview of the front panel LEDs and what they indicate. The following gives an overview of this section:

- 2.7.1 - Introducing the front panel LEDs on page 34
- 2.7.2 - The power LED (1 / 2) on page 35
- 2.7.3 - The power restart LED (R) on page 35
- 2.7.4 - The xDSL DCD LED (1 … 8) on page 36
- 2.7.5 - The station clock LED (CLK) on page 36
- 2.7.6 - The LAN LED (LAN) on page 36

2.7.1 Introducing the front panel LEDs

When all the connections are made and the Telindus 2400 is powered, the LEDs on the front panel reflect the actual status of the device.

The following figure shows the front panel LED indicators of the Telindus 2401/2421:



LED states

One front panel LED can reflect different status modes by the way it lights up. The front panel LEDs can light up as follows:

LED state	LED duty cycle	Description
continuously off	0 %	The LED never lights up.
continuously on	100 %	The LED lights up continuously.
blinking	50 %	The LED is as much lit as it is out.
flashing	20 %	The LED only lights up during 20% of the time.
mostly off	-	The LED occasionally lights up, without a fixed duty cycle.
mostly on	-	The LED occasionally goes out, without a fixed duty cycle.
monitoring	-	The LED lights up irregularly. For instance, it lights up on detection of a certain signal. I.e. it monitors this signal.

2.7.2 The power LED (1 / 2)

Since there are two power inputs, there are also two power LEDs (labelled 1 and 2). In case of a …

- Vdc model (two -48 Vdc inputs) …
  - LED 1 corresponds with the lower -48 Vdc input.
  - LED 2 corresponds with the upper -48 Vdc input.
- Vdc/Vac model (one 115/230 Vac input and one -48 Vdc input) …
  - LED 1 corresponds with the (lower) -48 Vdc input.
  - LED 2 corresponds with the 115/230 Vac input.

These LEDs only flash, blink or are on if a power supply is actually connected to the corresponding power supply connector.

The power LEDs indicate the following:

LED status	Description
continuously off	No input power is available.
flashing	The self test, performed during the boot sequence, failed or a hardware error occurred.
blinking	The Telindus 2400 operates in … • boot mode (e.g. because no loader and application software is present). • loader mode (e.g. because no application software is present or because you forced the Telindus 2400 in loader mode using the appropriate DIP switch). Refer to 19.1 - What is boot, loader and application software? on page 680 for more information on boot and loader mode.
continuously on	The Telindus 2400 is powered, the boot sequence was successful and the Telindus 2400 operates in application mode.

2.7.3 The power restart LED (R)

This LED reflects the status of the power circuit:

LED status	Description
continuously off	Normal condition.
continuously on	The power circuit has shut down due to an environmental error condition, e.g. temperature too high, failure of the fan(s), etc.

2.7.4 The xDSL DCD LED (1 … 8)

This LED reflects the status of each xDSL line:

LED status	Description
continuously off	No line signal is received from the remote modem. E.g. nothing is connected to the line.
blinking	A line signal is received from the remote modem and the handshake is in progress.
continuously on	A line signal is received from the remote modem and the handshake was successful. Data can be exchanged.

2.7.5 The station clock LED (CLK)

This LED reflects the status of the station clock:

LED status	Description
continuously off	• No (valid) station clock signal is present. or • A valid station clock signal is present, but the station clock is not used (e.g. the Telindus 2400 uses internal clocking).
continuously on	A valid station clock signal is present and the Telindus 2400 uses the station clock.

2.7.6 The LAN LED (LAN)

This LED reflects the link status and monitors the user data of the LAN interface:

LED status	Description
continuously off	Nothing is connected to the LAN interface.
monitoring	The Ethernet link is up and there is network activity on the LAN.
continuously on	The Ethernet link is up, but there is no network activity on the LAN.

3 DIP switches of the Telindus 2400

This chapter locates the DIP switches on the Telindus 2400 motherboard. It gives an overview of their function and it explains how to change their settings.

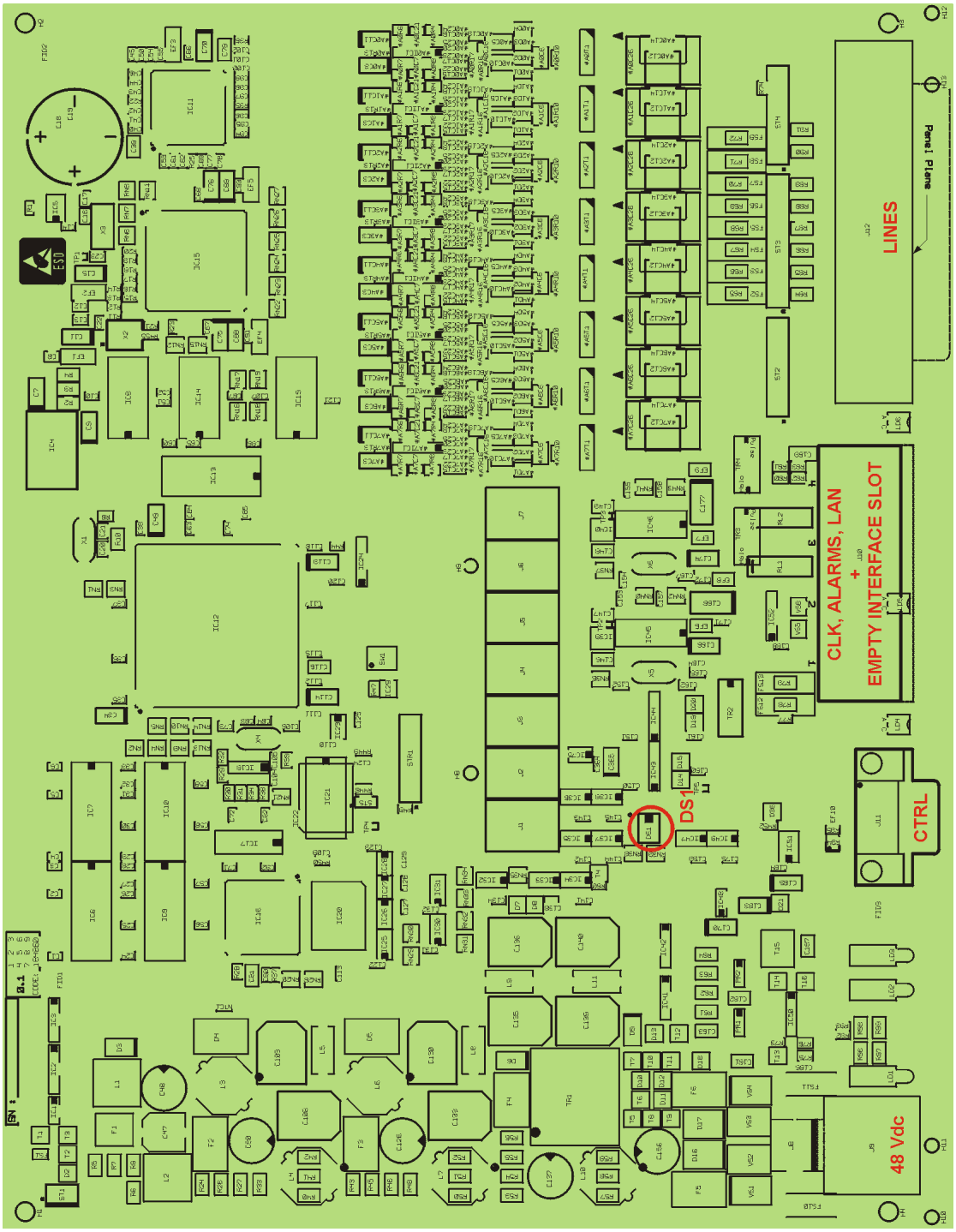
The following gives an overview of this chapter:

- 3.1 - The Telindus 2400 motherboard on page 38
- 3.2 - DIP switches of the Telindus 2400 on page 39
- 3.3 - Opening and closing the housing on page 40

Default settings are printed in **bold**.

3.1 The Telindus 2400 motherboard

The figure below shows the position of the DIP switches on the Telindus 2401/2421 motherboard:



3.2 DIP switches of the Telindus 2400

DIP switch bank DS1

The following table gives an overview of the DIP switches on DIP switch bank DS1:

DIP switch name	DS1 no.	Setting	Function
loader mode	1	**on**	Normal operation.
		off	Start up in loader mode. Refer to 19.2.5 - Downloading application software in loader mode on page 687.
load default configuration	2	**on**	Normal operation.
		off	Load default configuration. Refer to 6.6.4 - Loading the default configuration using a DIP switch on page 113.

Refer to 3.3 - Opening and closing the housing on page 40 to find out how to open the housing in order to change the DIP switch settings.

3.3 Opening and closing the housing

When you want to change the DIP switch settings, you have to open and close the housing of the Telindus 2400. This section explains how to do so.

Opening the housing

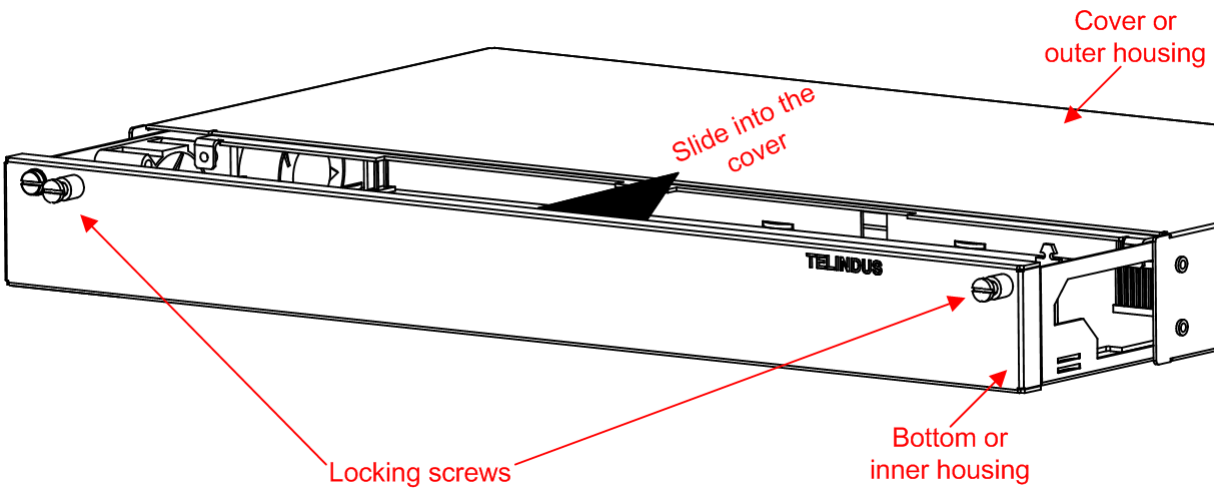
To open the housing of the Telindus 2400, proceed as follows:

Step	Action
1	Disconnect the external power supply.
2	Unscrew the two screws located at the front of the housing.
3	Slide the bottom out of the cover: • The bottom is the inner housing. This is the metal coloured part of the housing. • The cover is the outer housing. This is the dark grey coloured part of the housing. Refer to the figure below.

Closing the housing

To close the housing of the Telindus 2400, proceed as follows:

Step	Action
1	Slide the bottom in the cover: • The bottom is the inner housing. This is the metal coloured part of the housing. • The cover is the outer housing. This is the dark grey coloured part of the housing. Refer to the figure below.
2	Fasten the two screws located at the front of the housing.
3	Reconnect the external power supply.



4 Maintaining the Telindus 2400

Once you installed the Telindus 2400, you can proceed with the configuration of the Telindus 2400. You can do this using any of the maintenance or management tools introduced in 1.6 - Maintenance and management tools on page 15.

This chapter briefly highlights one of those tools: the Telindus Maintenance Application (TMA). It introduces TMA and describes how to start a session on the Telindus 2400. It also introduces the terminology concerning the management of a Telindus device. Furthermore, it explains why and how to add an object to the containment tree.

The following gives an overview of this chapter:

- 4.1 - Maintaining the Telindus 2400 with TMA on page 42
- 4.2 - Introducing the management terminology on page 48
- 4.3 - The objects in the Telindus 2400 containment tree on page 52
- 4.4 - Adding an object to the containment tree on page 56
- 4.5 - Telindus 2400 attribute overview on page 61

4.1 Maintaining the Telindus 2400 with TMA

First, this section introduces TMA. Then it describes how to start a session on the Telindus 2400. The following gives an overview of this section:

- 4.1.1 - What is TMA? on page 43
- 4.1.2 - How to connect TMA? on page 43
- 4.1.3 - Connecting with TMA through the control connector on page 44
- 4.1.4 - Connecting with TMA over an IP network on page 46

4.1.1 What is TMA?

TMA is the acronym for Telindus Maintenance Application. TMA is a free Windows software package that enables you to maintain the Telindus 2400, i.e. to access its configuration attributes and look at status, performance and alarm information using a user friendly graphical user interface.

TMA is an excellent tool for complete control of the Telindus access devices. When using TMA in combination with a network management system such as HP OpenView, complete networks can be managed from one central site.

Consult the TMA manual (PDF) to find out how to install TMA and to get acquainted with the user interface.

You will need a new version of the model file distribution if changes have been made to the attributes of the Telindus 2400. The most recent model files and TMA engine can always be downloaded from the Telindus web site at www.telindusproducts.com/TMA.

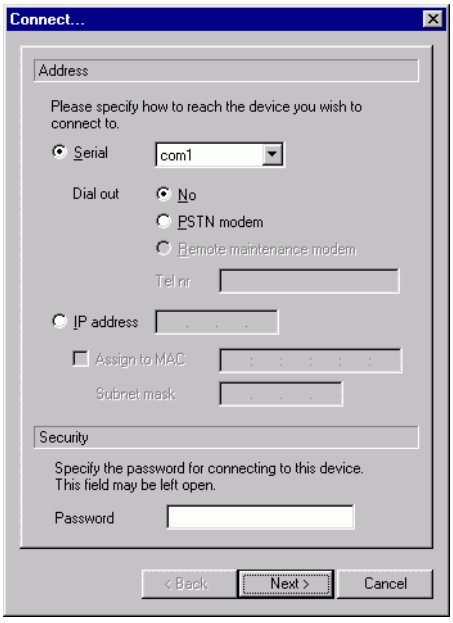
4.1.2 How to connect TMA?

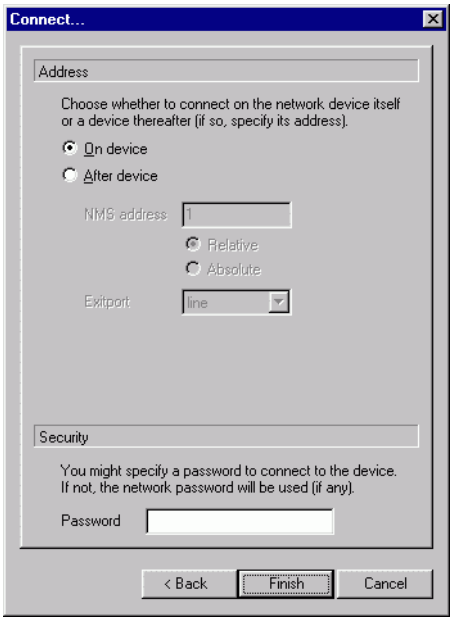
There are two ways to establish a connection between the computer running TMA and the Telindus 2400:

- through a serial connection, i.e. through the control connector of the Telindus 2400. Refer to 4.1.3 - Connecting with TMA through the control connector on page 44.
- through an IP connection, i.e. through the LAN connector of the Telindus 2400. Refer to 4.1.4 - Connecting with TMA over an IP network on page 46.

4.1.3 Connecting with TMA through the control connector

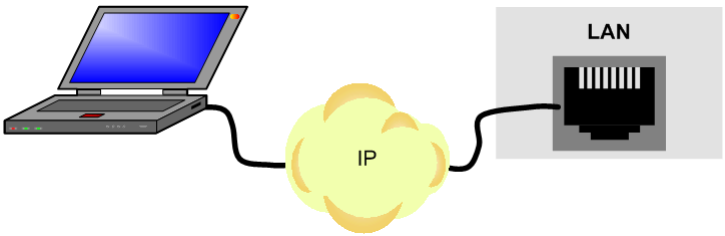
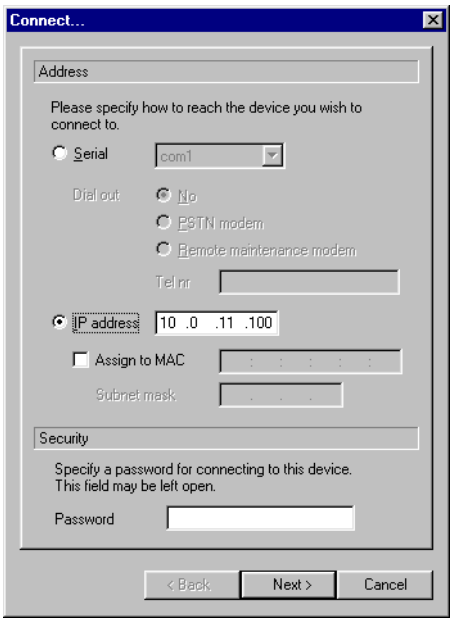
To established a connection between TMA and the Telindus 2400 through the control connector, proceed as follows:

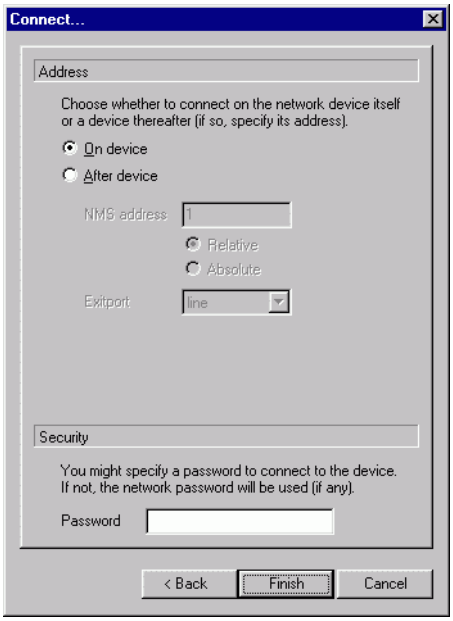
Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 2400.
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device…* • or press the short-cut key: Ctrl+N • or click on the *Connect to device* button: ⇒The *Connect…* (to a device) window is displayed.
4	In the *Connect…* (to a device) window, specify the following: • Select the option *Serial* and specify the COM port of your computer to which the Telindus 2400 is connected. • If previously a password has been configured in the Telindus 2400 then also fill in the password field. 
5	Click on the *Next* > button. ⇒The *Connect…* (select a device) window is displayed.

Step	Action
6	In the *Connect…* (select a device) window, select *On device*. 
7	Click on the *Finish* button.
8	After a couple of seconds, the attributes of the Telindus 2400 appear in the TMA window.

4.1.4 Connecting with TMA over an IP network

To established a connection between TMA and the Telindus 2400 over an IP network, proceed as follows:

Step	Action
1	Connect the IP network to … • the network port of your PC, • the LAN connector of the Telindus 2400. 
2	Start TMA.
3	In the TMA window, either … • select from the menu bar: *Connect* → *Device*… • or press the short-cut key: Ctrl+N • or press on the *Connect to device* button: ⇒The *Connect*… (to a device) window is displayed.
4	In the *Connect*… (to a device) window, specify the following: • Select the option *IP address* and enter the IP address of the Telindus 2400. • If a password has previously been configured in the Telindus 2400 then also fill in the password field. Before you are able to establish a connection over an IP network, you have to configure an IP address in the Telindus 2400. You can do this by first connecting TMA to the Telindus 2400 through the control connector, and then configuring an IP address. Refer to the 6.2 - Configuring IP addresses on page 87. 
5	Click on the *Next* > button. ⇒The *Connect*… (select a device) window is displayed.

Step	Action
6	In the *Connect…* (select a device) window, select *On device*. 
7	Click on the *Finish* button.
8	After a couple of seconds, the attributes of the Telindus 2400 appear in the TMA window.

4.2 Introducing the management terminology

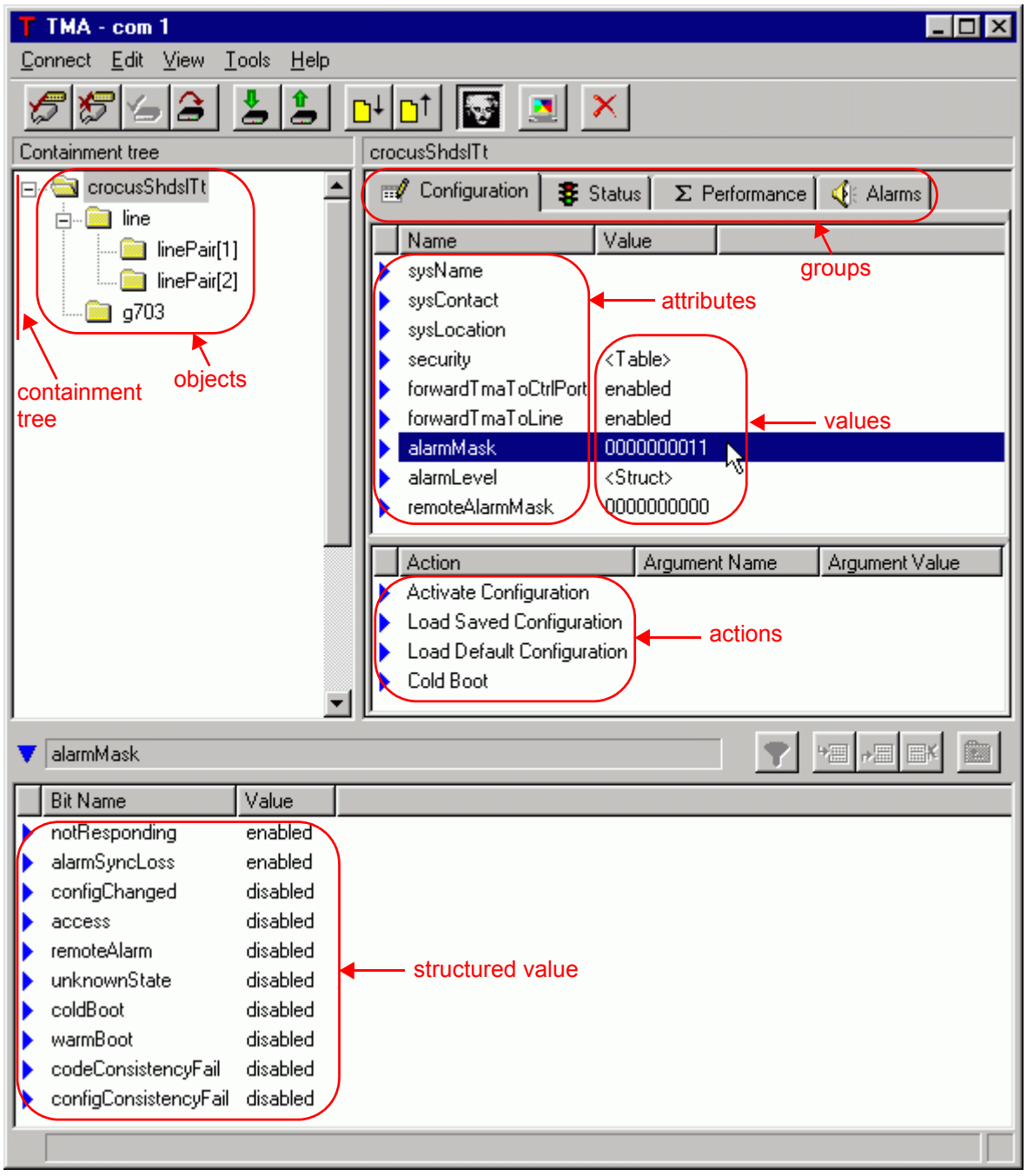
This section briefly introduces the terminology concerning the management of a Telindus device. It explains terms such as containment tree, group, object, attribute, value and action.

The following gives an overview of this section:

- 4.2.1 - Graphical representation of the containment tree on page 49
- 4.2.2 - Containment tree terminology on page 50

4.2.1 Graphical representation of the containment tree

The most comprehensible graphical representation of the containment tree is given in TMA. The following figure depicts the TMA window displaying a containment tree:



Refer to 4.2.2 - Containment tree terminology on page 50 for an explanation of the terms associated with the containment tree.

4.2.2 Containment tree terminology

Refer to 4.2.1 - Graphical representation of the containment tree on page 49 for a figure of a containment tree.

The following table explains the terminology associated with the containment tree:

Term	Description
containment tree	The containment tree represents the hierarchical structure of the Telindus 2400. It is composed of a number of objects that are ordered in a tree. This tree resembles a Windows directory structure: • it is also a levelled structure, with nodes which can be expanded or reduced. • the containment tree objects can be compared with file folders. • the objects contain attributes like file folders contain files.
object	An object represents a physical interface, an application or a combination of both. Each object has its own set of attributes.
parent and child object	Some objects are not present in the containment tree by default. If you want to use the features associated with such an object, then you have to add the object first. You always add an object under another object. The object you add is called the child object. The object under which you add this child object is called the parent object. Objects which you can add are also often referred to as *user-instantiatable objects*.
index name	Of some objects more than one object is present in the containment tree. The different objects are distinguished from one another by adding an index. E.g. linePair[1] and linePair[2], where 1 and 2 are the indexes. Also child objects are given an index (by the user when adding the object). An index name is also often referred to as *index*, *instance value* or *instance name*.
attribute	An attribute is a parameter related to a certain object. It has a certain value.
value	An attribute has a certain value which is … • changeable in case of a configuration attribute (provided you have write access). • read only in case of a status, performance and alarm attribute.
structured value	Some attribute values contain underlying values: a structured value. These values are displayed in the structured value window. If an attribute contains structured values, then a bit string, <Table> or <Struct> is displayed after the attribute: • a bit string is a series of bits. The value of each of these bits can be 0 or 1, on or off, enabled or disabled. • a table contains columns and rows. Each column contains an attribute (which, on its turn, can have a structured value). Each row is an entry in the table. • a structure contains columns but only one row. A structure could be compared to an attribute which contains several “sub-attributes”. A structured value is also often referred to as *bit string*, *table*, *structure* or *complex value*.

Term	Description
element	An element is an attribute within a structured value. In other words, they could be considered as “sub-attributes”.
group	Groups assemble a set of attributes related by functionality. There are four groups in TMA, which correspond with the four tabs in the attribute window: • configuration, • status, • performance, • alarms.
action	A group in combination with an object may have actions assigned to them. These actions are displayed in the action window.

4.3 The objects in the Telindus 2400 containment tree

The following table lists the different objects of the Telindus 2400 containment tree. It also specifies whether the objects are present by default, whether you have to add them yourself or whether they are added automatically.

Object	Remarks
> telindus24xx	Depending on the Telindus 2400 model, the name of this object can be telindus2401, telindus2402, telindus2403, telindus2421, telindus2422, telindus2423. Refer to 1.4 - Telindus 2400 series overview on page 9.
>> lanInterface	
>>> atm	
>> 4pEth	This object is only present if the 4 port Ethernet interface module is inserted in the empty interface slot.
>> hexE1	This object and all its sub-objects is only present if the 6E1 interface module is inserted in the empty interface slot.
>>> e1[E1_x]	Depending on the hardware configuration of the 6E1 interface, 6 or 8 e1[E1_x] objects are present. I.e. from e1[E1_1] up to e1[E1_6] or e1[E1_8]. Refer to the 6E1 interface manual (PDF) for more information on its hardware configuration.
>>>> atm	
>> e3T3	This object is only present if the E3/T3 interface module is inserted in the empty interface slot.
>>> e3T3[E3T3_x]	Depending on the E3/T3 interface version (single or dual), 1 or 2 e3T3[E3T3_x] objects are present.
>>>> atm	
>> bundle	
>>> imaGroup[ ]	This object is not present by default, it has to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.
>> dslInterfaces	
>>> interface[dsl_x]	Depending on the Telindus 2400 model, 8, 16 or 24 interface[dsl_x] objects are present. I.e. interface[dsl_1] up to interface[dsl_8], interface[dsl_16] or interface[dsl_24].
>>>> line	In case of a Telindus 2400 ADSL model, this object is always present. In case of a Telindus 2400 SHDSL model, this object is not present by default. It only appears when the necessary profiles have been configured and applied on the SHDSL interface.

Object	Remarks
>>>>> linePair	
>>>> repeater	This object applies on a Telindus 2400 SHDSL model only. It is not present by default, it only appears when an SHDSL repeater is detected on the line.
>>>>> linePair	
>>>> end	In case of a Telindus 2400 ADSL model, this object is always present. In case of a Telindus 2400 SHDSL model, this object is not present by default. It only appears when a remote SHDSL modem is detected on the line.
>>>>> linePair	
>>>> atm	
>> profiles	
>>> xdsl	
>>>> shdsl_default	These objects apply on a Telindus 2400 SHDSL model only. The default profile object is always present (the default object). However, additional profile objects can be added. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63.
>>>> shdsl[ ]	
>>>> adsl_default	These objects apply on a Telindus 2400 ADSL model only. The default profile object is always present (the default object). However, additional profile objects can be added. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63.
>>>> adsl[ ]	
>>> atm	
>>>> pvc_default	The default profile object is always present (the default object). However, additional profile objects can be added. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63.
>>>> pvc[ ]	
>>> forwardingMode	
>>>> routing_default	The default profile object is always present (the default object). However, additional profile objects can be added. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63.
>>>> routing[ ]	
>>>> bridging_default	
>>>> bridging[ ]	
>>> policy	
>>>> priority	

Object	Remarks
>>>>> priorityPolicy[ ]	This object is not present by default, it has to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.
>>>> traffic	
>>>>> ipTrafficPolicy[ ]	These objects are not present by default, they have to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.
>>>>> bridgingTrafficPolicy[ ]	
>>> lineConfiguration	
>>>> shdslAtm_default	The default profile object is always present (the default object). However, additional profile objects can be added. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63.
>>>> shdslAtm[ ]	
>>>> adslAtm_default	
>>>> adslAtm[ ]	
>> atm	
>> ip	
>>> router	
>>>> defaultNat	
>>>> tunnels	
>>>> routingFilter[ ]	These objects are not present by default, they have to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.
>>>> manualSA[ ]	
>> bridge	
>>> bridgeGroup	
>>> vpnBridgeGroup[ ]	These objects are not present by default, they have to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.
>>> accessList[ ]	
>> alarmContacts	
>> snmp	
>> management	
>>> loopBack	
>>> usrLoopBack[ ]	This object is not present by default, it has to be added. Refer to 4.4 - Adding an object to the containment tree on page 56.

Object	Remarks
>> fileSystem	
>> operatingSystem	

4.4 Adding an object to the containment tree

This section explains why and how you can add an object to the containment tree. It then explains why and how to refer to this object.

The following gives an overview of this section:

- 4.4.1 - Why add an object to the containment tree? on page 57
- 4.4.2 - How to add an object to the containment tree? on page 58
- 4.4.3 - Referring to an added object on page 60

4.4.1 Why add an object to the containment tree?

Why can you add an object to the containment tree?

Some objects are not present in the containment tree by default but you can add them yourself because …

- in this way the containment tree remains clear and surveyable,
- you possibly do not need the functions associated with such an object,
- you possibly need several of these objects so you can add as many objects as you like.

When do you have to add an object to the containment tree?

If you want to use the features associated with such an object, then you have to add the object first.

Which objects can be added to the containment tree?

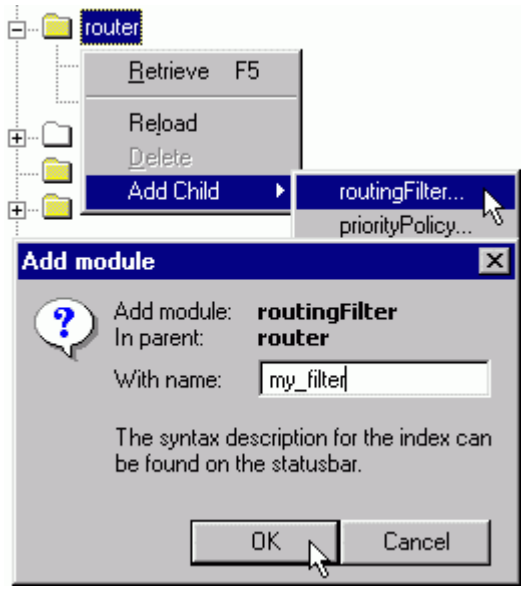
Section 4.3 - The objects in the Telindus 2400 containment tree on page 52 gives you an overview of all the objects in the containment tree. It also tells you which objects have to be added before you can use them.

4.4.2 How to add an object to the containment tree?

The section shows you, for each maintenance tool, how to add an object to the containment tree. The following section, 4.4.3 - Referring to an added object on page 60, shows you how you can “refer” to this added object somewhere else in the containment tree.

Adding an object in TMA

Step	Action
1	Right click on the parent object (e.g. router). ⇒A pop-up menu appears.
2	In the pop-up menu, select *Add Child…* and select the child object you want to add (e.g. routingFilter). ⇒A pop-up window appears.
3	In the pop-up window, type the index name (i.e. the instance value) for the child object (e.g. my_filter) and click on *OK*. ⇒The new child object is created (e.g. routingFilter[my_filter]).



Adding an object in (TMA) CLI

Step	Action
1	Enter the parent object (e.g. `select router`).
2	Type the following command: `set {select childObjectName[instanceValue]{}}` where `instanceValue` is a string of your choice. (e.g. `set {select routingFilter[my_filter]{}}`) ⇒The new child object is created.

Adding an object in ATWIN

Step	Action
1	Enter the parent object (e.g. go to the router object and press the enter key). ⇒The ATWIN window shows the sub-objects and attributes of the parent object.
2	Go to the line displaying the string `<CREATE INSTANCE>` and the name of the object you want to add (e.g. `routingFilter <CREATE INSTANCE>`) and press the enter key. ⇒A new window appears, displaying the string `Give the instanceValue`.
3	Press the enter key and type the index name (i.e. the instance value) for the child object (e.g. my_filter) and press the enter key again. ⇒The new child object is created (e.g. `>.routingFilter [name:my_filter])`.

Adding an object in the Web Interface

Step	Action
1	Enter the parent object (e.g. select the router object and double-click it or click on *Open*). ⇒The Web Interface window shows the sub-objects and attributes of the parent object.
2	Select the line displaying the string `<CREATE INSTANCE>` and the name of the object you want to add (e.g. `routingFilter <CREATE INSTANCE>`) and double-click it or click on *Open*. ⇒A new window appears, displaying the string `Give the instanceValue`.
3	Type the index name (i.e. the instance value) for the child object (e.g. my_filter) and click on *exit*. ⇒The new child object is created (e.g. `>.routingFilter [name:my_filter])`.

4.4.3 Referring to an added object

What is referring to an added object?

If at a certain place in the containment tree you want to apply the function associated with an object you added, then you have to refer to this object.

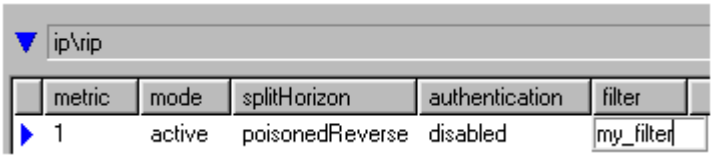
How to refer to an added object?

Some attributes allow you to enter the index name (i.e. the instance value you assigned to the object) of an added object. By doing so, the function associated with this object is applied there.

Example

Suppose you create a routingFilter object with the index name my_filter. The containment tree then looks as follows:

Now, you want to use this filter on the LAN interface. In that case, in the ip/rip structure in the lanInterface object, enter the index name of the routingFilter object under the element “filter”. This looks as follows:



4.5 Telindus 2400 attribute overview

The reference part of this manual explains all the attributes of the Telindus 2400. One chapter describes one group of attributes:

- chapter 13 - Configuration attributes on page 297,
- chapter 14 - Status attributes on page 473,
- chapter 15 - Performance attributes on page 579,
- chapter 16 - Alarm attributes on page 641.

5 Configuring the Telindus 2400 - the concept of profiles

The configuration of the Telindus 2400 is based on profiles. This means that in order to configure the xDSL lines, the encapsulation on these lines and the routing and/or bridging functionality, you have to create and apply profiles. Therefore, this chapter introduces the concept of profiles and describes how to create and apply them in order to configure the Telindus 2400.

The following gives an overview of this chapter:

- 5.1 - Explaining profiles on page 64
- 5.2 - How to create a configuration using profiles? on page 74

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

5.1 Explaining profiles

This section introduces the concept of profiles. The following gives an overview of this section:

- 5.1.1 - What is a profile? on page 65
- 5.1.2 - Which profiles are there? on page 66
- 5.1.3 - What is a default and a custom profile? on page 68
- 5.1.5 - How to link the different profiles together? on page 70
- 5.1.6 - Linking the different profiles together - an example on page 73

5.1.1 What is a profile?

What is a profile?

On Telindus products such as the modems (e.g. the Crocus SHDSL, etc.), a certain physical interface always has a corresponding set of configuration attributes. This is no longer the case on the Telindus 2400.

The Telindus 2400 makes use of (configuration) profiles. This means that you can create one or more profiles and apply them on one or more interfaces. For example, you can create only one xDSL profile and apply this profile on all xDSL lines.

Advantages of profiles

The advantages of using profiles is that if several interfaces require the same configuration, you do not have to configure these interfaces over and over again. Instead, you create one profile and apply it to all interfaces.

Another advantage of using profiles is that you can decide in advance …

- which application you intend to offer. E.g. routing without RIP, routing with RIP enabled, bridging, bridging with Spanning Tree enabled, etc.
- which encapsulation you intend to offer for these applications.
- which line parameters you intend to offer for each customer. E.g. which speed, which SHDSL or ADSL standard, etc.

Then you can combine these profiles in several configurations. E.g. you can combine the same routing forwarding profile with different encapsulation profiles to allow compatibility with the various default settings of different types of CPE equipment. Or you can combine the same application and encapsulation profile with different xDSL profiles to offer different line speeds.

Summarised, profiles offer you flexibility. They allow you to prepare several configurations in advance and …

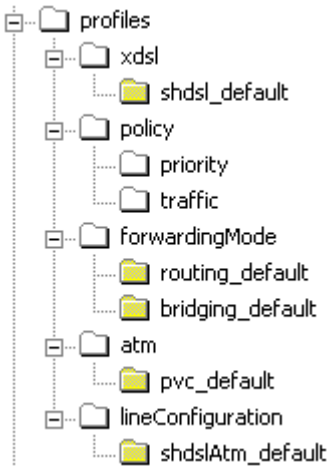
- activate these configurations at the time they are needed.
- switch between configurations depending on the needs of the customer.

5.1.2 Which profiles are there?

The following profiles exist:

Profile	Description
xDSL	Using this profile you can configure the xDSL (ADSL or SHDSL) related parameters of the connection. So in this profile you will find configuration attributes such as speed, retrain, etc. The location of the xDSL profiles in the containment tree is: telindus24xx/profiles/xdsl
ATM PVC	Using this profile you can configure the ATM PVC related parameters of the connection. So in this profile you will find configuration attributes such as vpi, vci, qos, etc. The location of the ATM PVC profiles in the containment tree is: telindus24xx/profiles/atm
forwarding mode	Using these profiles you can configure the routing and/or bridging related parameters of the connection. So in these profiles you will find configuration attributes such as algorithm, method, trafficShaping, etc. The location of the forwarding profiles in the containment tree is: telindus24xx/profiles/forwardingMode
policy	Using these profiles you can configure the priority and traffic policy related parameters of the connection. So in these profiles you will find configuration attributes such as ip, bridging, priorityPolicy, etc. The location of the policy profiles in the containment tree is: telindus24xx/profiles/policy
line configuration	Using this profile you actually set up the line configuration by linking the xDSL and ATM PVC profile together (the forwarding profile is already included in the ATM PVC profile). Once you did this, you can apply the line configuration profile on an xDSL line. The location of the line configuration profiles in the containment tree is: telindus24xx/profiles/lineConfiguration

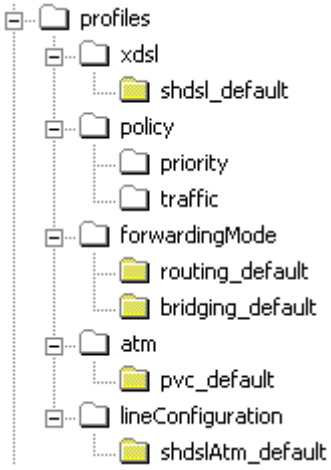
The following screenshot shows the different profile objects in the Telindus 2400 containment tree:



5.1.3 What is a default and a custom profile?

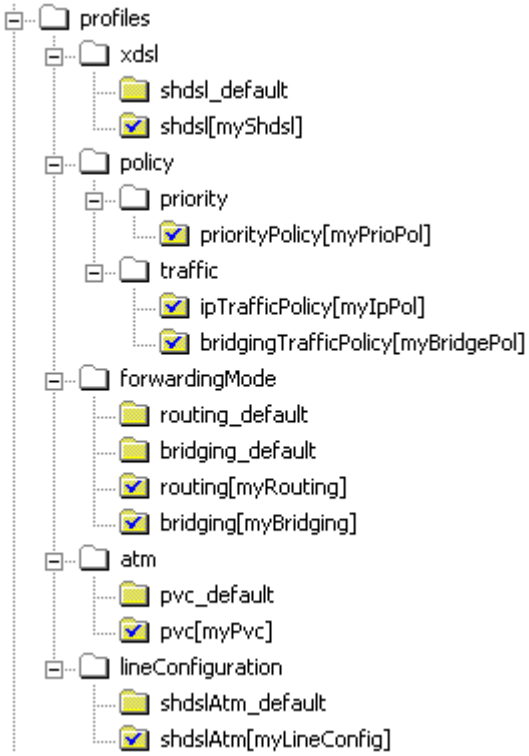
The default profile

The xdsl, atm, forwardingMode and lineConfiguration objects always contain a sub-object which has the string "default" in its name. These are what we call the default profiles.



The custom profile

Under the xdsl, atm, forwardingMode, policy/priority, policy/traffic and lineConfiguration objects you can add additional sub-objects. These are what we call the custom profiles.

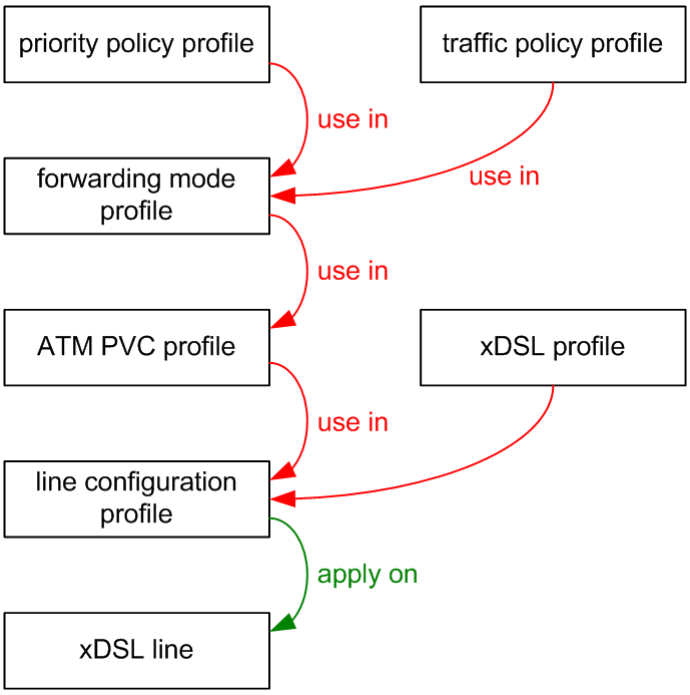


The profile attributes

The default and custom profiles on their turn contain the actual configuration attributes. Change these attributes to create a specific configuration profile.

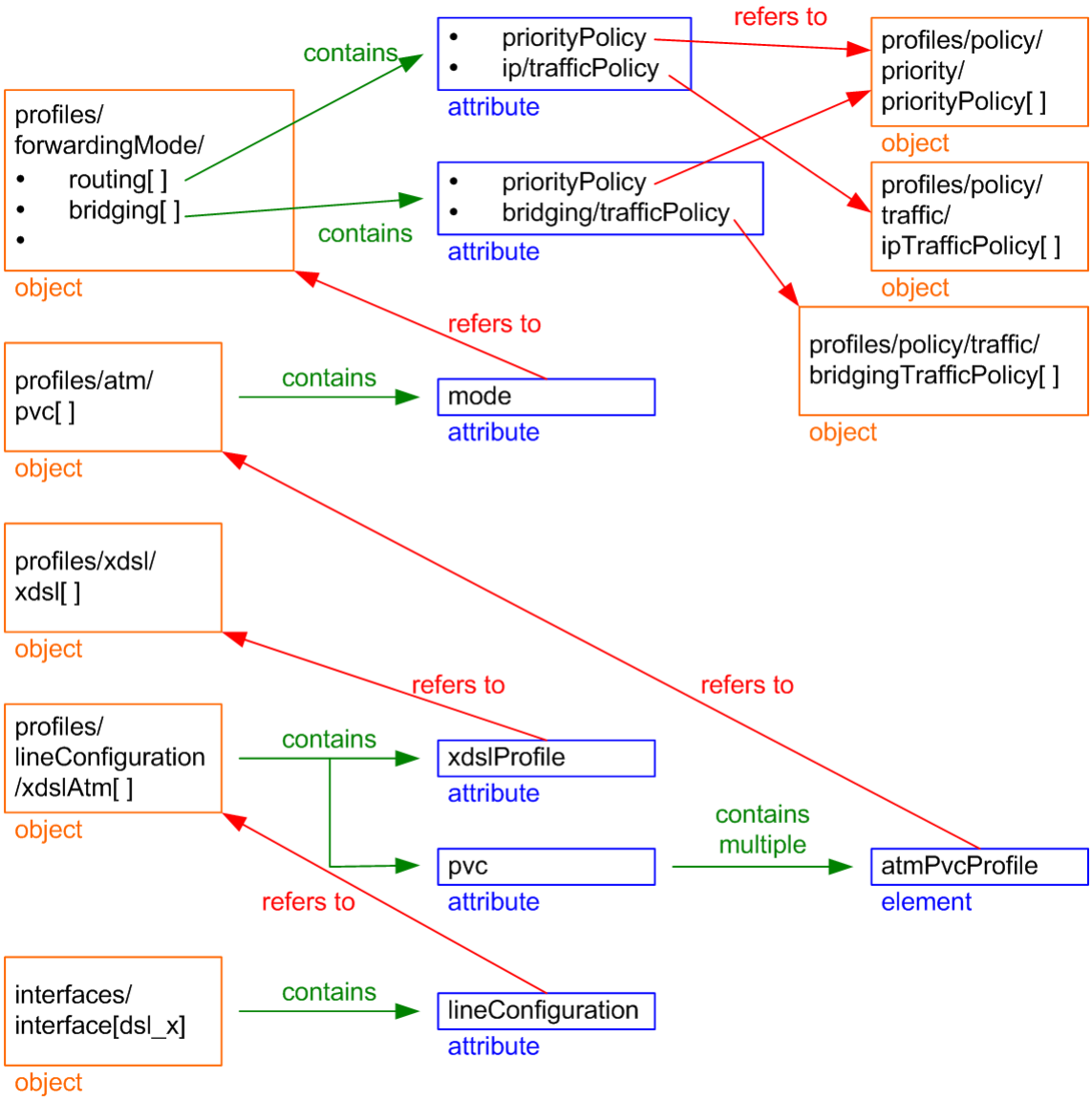
5.1.4 How do the different profiles relate to each other?

Setting up profiles only is not enough. In some way, you have to “link” the xDSL, ATM PVC, forwarding, policy and line configuration profiles together. Before a description is gives of how exactly these profiles are linked together (refer to 5.1.5 - How to link the different profiles together? on page 70), the following figure gives you a schematic overview of how the different profiles relate to each other.



5.1.5 How to link the different profiles together?

As said before, setting up profiles only is not enough. In some way, you have to “link” the xDSL, ATM PVC, forwarding, policy and line configuration profiles together (also refer to 5.1.4 - How do the different profiles relate to each other? on page 69). This is done by “referring” to these profiles in specific places in the containment tree. The following shows you schematically in which place in the containment tree you have to refer to which profile:



The priorityPolicy[ ] object

The profiles/policy/priority/priorityPolicy[ ] object contains the priority policy profile configuration attributes. Configure these attributes to create a specific priority policy profile.

The ipTrafficPolicy[ ] object

The profiles/policy/traffic/ipTrafficPolicy[ ] object contains the IP traffic policy profile configuration attributes. Configure these attributes to create a specific IP traffic policy profile. The IP traffic policy is a traffic policy specifically for routed data.

The bridgingTrafficPolicy[ ] object

The profiles/policy/traffic/bridgingTrafficPolicy[ ] object contains the bridging traffic policy profile configuration attributes. Configure these attributes to create a specific bridging traffic policy profile. The bridging traffic policy is a traffic policy specifically for bridged data.

The routing_default and routing[ ] objects

The profiles/forwardingMode/routing_default and routing[ ] objects contain the …

- routing forwarding configuration attributes. Configure these attributes to create a specific routing forwarding profile.
- attribute priorityPolicy. Using this attribute you can specify which priority policy profile you want to use in the routing forwarding profile. The priority policy profile is an object that you (created and) configured earlier.
- attribute ip which, on its turn, contains the element trafficPolicy. Using this element you can specify which IP traffic policy profile you want to use in the routing forwarding profile. The IP traffic policy profile is an object that you (created and) configured earlier.

The bridging_default and bridging[ ] objects

The profiles/forwardingMode/bridging_default and bridging[ ] objects contain the …

- bridging forwarding configuration attributes. Configure these attributes to create a specific bridging forwarding profile.
- attribute priorityPolicy. Using this attribute you can specify which priority policy profile you want to use in the bridging forwarding profile. The priority policy profile is an object that you (created and) configured earlier.
- attribute bridging which, on its turn, contains the element trafficPolicy. Using this element you can specify which bridging traffic policy profile you want to use in the bridging forwarding profile. The bridging traffic policy profile is an object that you (created and) configured earlier.

The pvc_default and pvc[ ] objects

The profiles/atm/pvc_default and pvc[ ] objects contain the …

- ATM PVC configuration attributes. Configure these attributes to create a specific ATM PVC profile.
- attribute mode. Using this attribute you can specify which forwarding profile you want to use in the ATM PVC profile. The forwarding profile is an object that you (created and) configured earlier.

The xdsl_default and xdsl[ ] objects

The profiles/xdsl/xdsl_default and xdsl[ ][1] objects contain the xDSL configuration attributes. Configure these attributes to create a specific xDSL profile.

The xdslAtm_default and xdslAtm[ ] objects

The profiles/lineConfiguration/xdslAtm_default and xdslAtm[ ][2] objects contain the attributes …

- xdslProfile[3]. Using this attribute you can specify which xDSL profile you want to use in the line configuration profile. The xDSL profile is an object that you (created and) configured earlier.
- pvc which, on its turn, contains the element atmPvcProfile. Using this element you can specify which ATM PVC profile you want to use in the line configuration profile. The ATM PVC profile is an object that you (created and) configured earlier.

The interface[dsl_x] objects

The dslInterfaces/interface[dsl_x][4] objects contain the attribute lineConfiguration. Using this attribute you specify which line configuration profile you want to apply on this particular xDSL line. This line configuration profile is an object that you (created and) configured earlier.

---

1. Where xdsl_default and xdsl[ ] are called …
   shdsl_default and shdsl[ ] in case of a Telindus 2400 SHDSL model.
   adsl_default and adsl[ ] in case of a Telindus 2400 ADSL model.
2. Where xdslAtm_default and xdslAtm[ ] are called …
   shdslAtm_default and shdslAtm[ ] in case of a Telindus 2400 SHDSL model.
   adslAtm_default and adslAtm[ ] in case of a Telindus 2400 ADSL model.
3. Where xdslProfile is called …
   shdslProfile in case of a Telindus 2400 SHDSL model.
   adslProfile in case of a Telindus 2400 ADSL model.
4. Where x ranges from 1 up to 8, 1 up to 16 or 1 up to 24, depending on the Telindus 2400 model.

5.1.6 Linking the different profiles together - an example

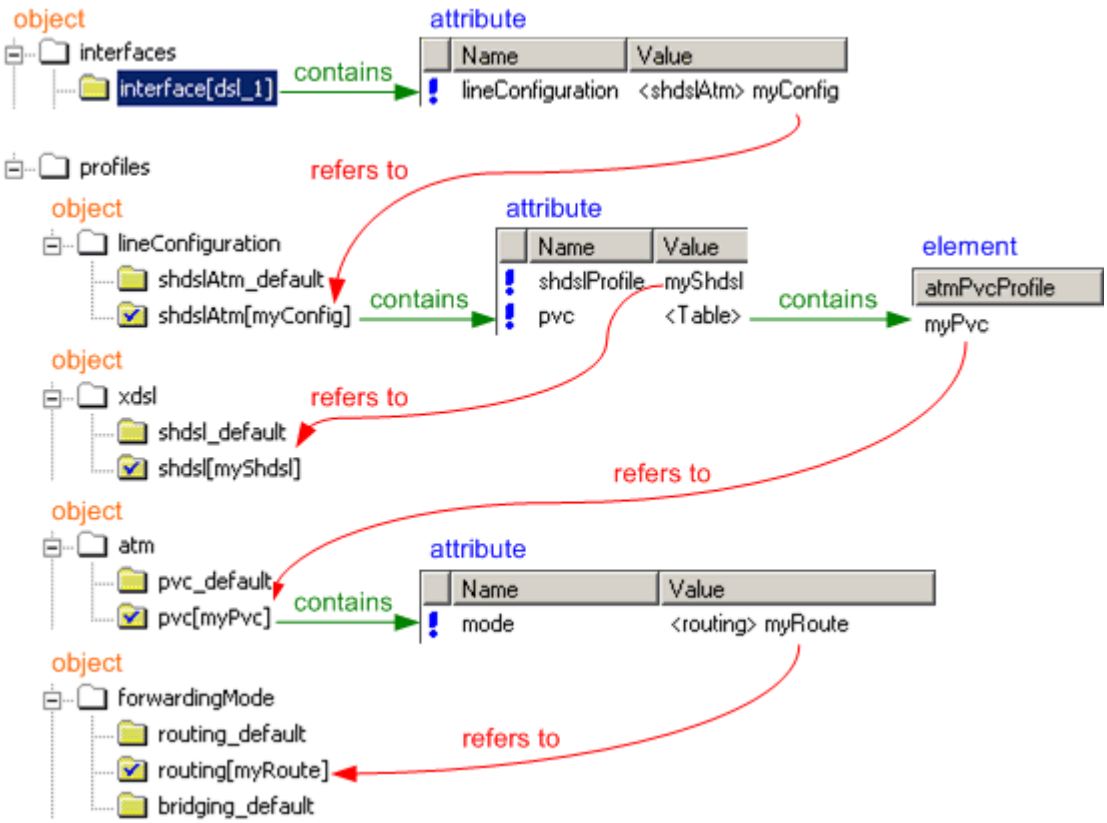
Suppose you create the following custom profiles:

- a custom routing forwarding profile: profiles/forwardingMode/routing[myRoute].
- a custom ATM PVC profile: profiles/atm/pvc[myPvc].
- a custom xDSL profile: profiles/xdsl/shdsl[myShdsl].
- a custom line configuration profile: profiles/lineConfiguration/shdslAtm[myConfig].

In order to make up a complete configuration, you have to apply …

- the custom routing forwarding profile routing[myRoute] on the custom ATM PVC profile pvc[myPvc].
- both the custom ATM PVC profile pvc[myPvc] and the custom xDSL profile shdsl[myShdsl] on the custom line configuration profile shdslAtm[myConfig].
- the custom line configuration profile shdslAtm[myConfig] on an SHDSL line, e.g. SHDSL line 1: interface[dsl_1].

Configure this as follows:



5.2 How to create a configuration using profiles?

Refer to 5.1 - Explaining profiles on page 64 for an introduction on profiles.

If you want to create a complete configuration using profiles, then proceed as follows:

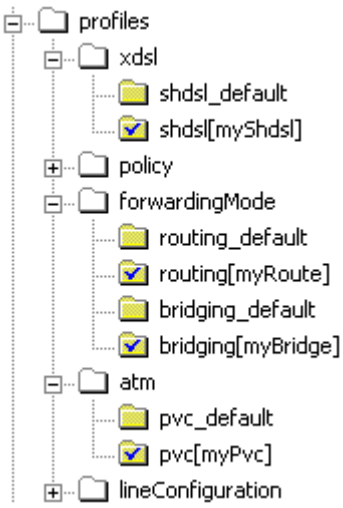
Step	Action
1	Create an xDSL, ATM PVC and forwarding profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75. You can also create priority and traffic policy profiles and apply these profiles on a forwarding profile. However, this is not essential for the configuration of an xDSL line and therefore not explained here. Refer to 9.7 - Configuring traffic and priority policy on the router on page 207.
2	Apply the forwarding profile on the ATM PVC profile. Refer to 5.2.2 - How to apply the forwarding profile? on page 77.
3	Create a line configuration profile. Refer to 5.2.3 - How to create a line configuration profile? on page 79.
4	Apply the xDSL and ATM PVC profiles on the line configuration profile. Refer to 5.2.4 - How to apply the xDSL and ATM PVC profiles? on page 80.
5	Apply the line configuration profile on an xDSL line. Refer to 5.2.5 - How to apply the line configuration profile? on page 82.

5.2.1 How to create an xDSL, ATM PVC and forwarding profile?

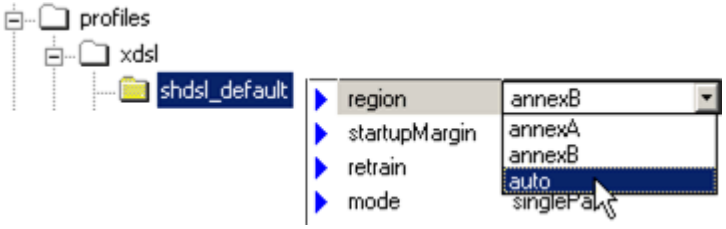
Refer to 5.2 - How to create a configuration using profiles? on page 74 for an overview on how to create a configuration. To give you an idea of where you are in the process, the following also gives a quick overview:

- → **Create an xDSL, ATM PVC and forwarding profile.** ← **You are here.**
- Apply the forwarding profile on the ATM PVC profile.
- Create a line configuration profile.
- Apply the xDSL and ATM PVC profiles on the line configuration profile.
- Apply the line configuration profile on an xDSL line.

In order to create an xDSL, ATM PVC and forwarding profile, proceed as follows:

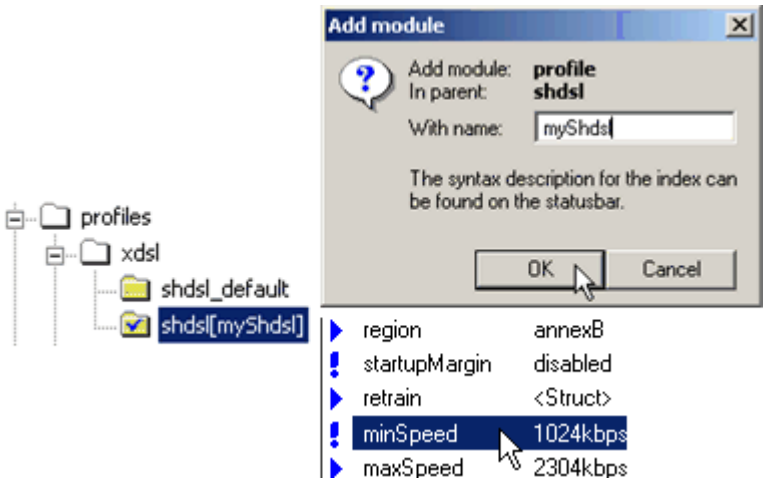
Step	Action
1	In the Telindus 2400 containment tree, go to the object … • profiles/xdsl if you want to create (an) xDSL profile(s). • profiles/atm if you want to create (an) ATM PVC profile(s). • profiles/forwardingMode if you want to create (a) forwarding profile(s).
2	Under these objects, you find a sub-object with the string "default" in its name. This is the default profile. If you want to set up … • a default profile, then configure the attributes in the "default" sub-object. • a custom profile, then first add a sub-object (refer to 4.4 - Adding an object to the containment tree on page 56). Then configure the attributes in this "custom" sub-object.  Refer to … • 13.10.1 - SHDSL profile configuration attributes on page 355 for more information on the configuration attributes of the SHDSL profile. • 13.10.2 - ADSL profile configuration attributes on page 362 for more information on the configuration attributes of the ADSL profile. • 13.10.3 - ATM PVC profile configuration attributes on page 369 for more information on the configuration attributes of the ATM PVC profile. • 13.10.4 - Forwarding profile configuration attributes on page 378 for more information on the configuration attributes of the forwarding profile.

Example: creating a default profile



Suppose you want to create one SHDSL profile for all SHDSL lines. In that case it is sufficient to configure the configuration attributes in the profiles/xdsl/shdsl_default object. E.g. set the region attribute to auto.

Example: creating a custom profile



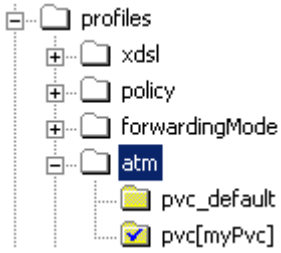
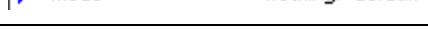
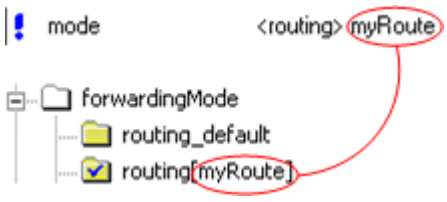
Suppose that for most of the SHDSL lines the default SHDSL profile suffices, but that one SHDSL line requires a specific configuration. In that case, you can create a custom SHDSL profile for that particular SHDSL line. Do this by adding an SHDSL profile object and configuring the configuration attributes in this object. E.g. suppose you add an SHDSL profile object with index name myShdsl and that in this object you set the startupMargin attribute to disabled and the minSpeed attribute to 1024kbps.

5.2.2 How to apply the forwarding profile?

Refer to 5.2 - How to create a configuration using profiles? on page 74 for an overview on how to create a configuration. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create an xDSL, ATM PVC and forwarding profile.
- → **Apply the forwarding profile on the ATM PVC profile.** ← **You are here.**
- Create a line configuration profile.
- Apply the xDSL and ATM PVC profiles on the line configuration profile.
- Apply the line configuration profile on an xDSL line.

In order to apply the forwarding profile on the ATM PVC profile, proceed as follows:

Step	Action
1	Go to the ATM PVC profile you previously created (refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75). 
2	Go to the attribute mode. 
3	First select the type of forwarding you want to apply. Do this by using the first part of the value field. If you want to apply … • a routing forwarding profile, then select routing. • a bridging forwarding profile, then select bridging. • ATM switching, then select atmSwitching. Note that ATM switching does not have to be configured in a profile, but in the ATM switching table. So in that case, the second part of the higherLayerProtocol attribute has no function (see below).
4	Then type the name of the forwarding profile you want to apply. Do this in the second part of the value field. If you want to apply …  • a default forwarding profile, then type the string “default”. • a custom forwarding profile, then type the index name of the custom forwarding object you previously added (refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75). E.g. type the string “myRoute” if the custom forwarding object that you added is called profiles/forwardingMode/routing[myRoute]. ATM switching does not have to be configured in a profile, but in the ATM switching table. So in case you set the first part of the higherLayerProtocol attribute to atmSwitching, then the second part of the higherLayerProtocol attribute has no function. Refer to 11.3 - Configuring ATM switching on page 256 for more information.

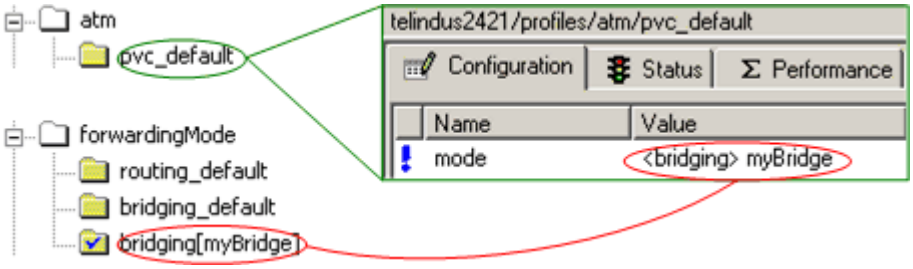
Example: applying a forwarding profile on an ATM PVC profile

Suppose you have …

- a default ATM PVC profile (profiles/atm/pvc_default)
- a custom bridging forwarding profile (profiles/forwardingMode/bridging[myBridge])

… and want to apply the custom bridging forwarding profile on the default ATM PVC profile.

In that case configure the mode attribute in the default ATM PVC profile as follows:

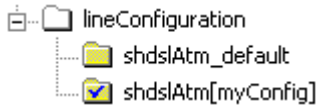


5.2.3 How to create a line configuration profile?

Refer to 5.2 - How to create a configuration using profiles? on page 74 for an overview on how to create a configuration. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create an xDSL, ATM PVC and forwarding profile.
- Apply the forwarding profile on the ATM PVC profile.
- → **Create a line configuration profile.** ← **You are here.**
- Apply the xDSL and ATM PVC profiles on the line configuration profile.
- Apply the line configuration profile on an xDSL line.

In order to create a line configuration profile, proceed as follows:

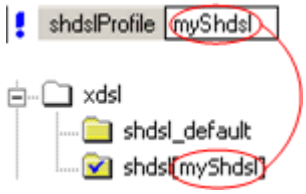
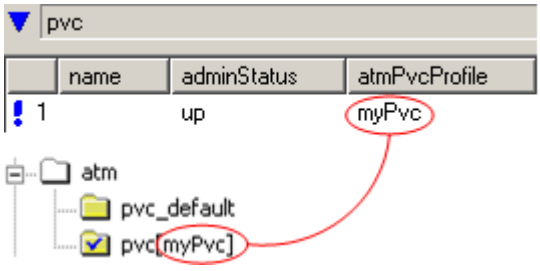
Step	Action
1	In the Telindus 2400 containment tree, go to the object profiles/lineConfiguration.
2	Under this object, you find a sub-object with the string "default" in its name. This is the default profile.  If you want to set up … • a default profile, then configure the attributes in the "default" sub-object. • a custom profile, then first add a sub-object (refer to 4.4 - Adding an object to the containment tree on page 56). Then configure the attributes in this "custom" sub-object.

5.2.4 How to apply the xDSL and ATM PVC profiles?

Refer to 5.2 - How to create a configuration using profiles? on page 74 for an overview on how to create a configuration. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create an xDSL, ATM PVC and forwarding profile.
- Apply the forwarding profile on the ATM PVC profile.
- Create a line configuration profile.
- → **Apply the xDSL and ATM PVC profiles on the line configuration profile.** ← **You are here.**
- Apply the line configuration profile on an xDSL line.

In order to apply the xDSL and ATM PVC profiles on the line configuration profile, proceed as follows:

Step	Action
1	**Apply the xDSL profile** Go to the line configuration profile you previously created (refer to 5.2.3 - How to create a line configuration profile? on page 79).
2	Go to the attribute shdslProfile.
3	Type the name of the xDSL profile you want to apply as value of the shdslProfile attribute. If you want to apply …  • a default xDSL profile, then type the string “default”. • a custom xDSL profile, then type the index name of the custom xDSL object you previously added (refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75). E.g. type the string “myShdsl” if the custom SHDSL object that you added is called profiles/xdsl/shdsl[myShdsl].
4	**Apply the ATM PVC profile** Go to the attribute pvc.
5	Add a line for every ATM Permanent Virtual Circuit you want to create. So if you want to create only 1 ATM PVC, then add 1 line to the pvc table.
6	Type the name of the ATM PVC profile you want to apply as value of the atmPvcProfile element. If you want to apply …  • a default ATM PVC profile, then type the string “default”. • a custom ATM PVC profile, then type the index name of the custom ATM PVC object you previously added (refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75). E.g. type the string “myPvc” if the custom ATM PVC object that you added is called profiles/atm/pvc[myPvc].

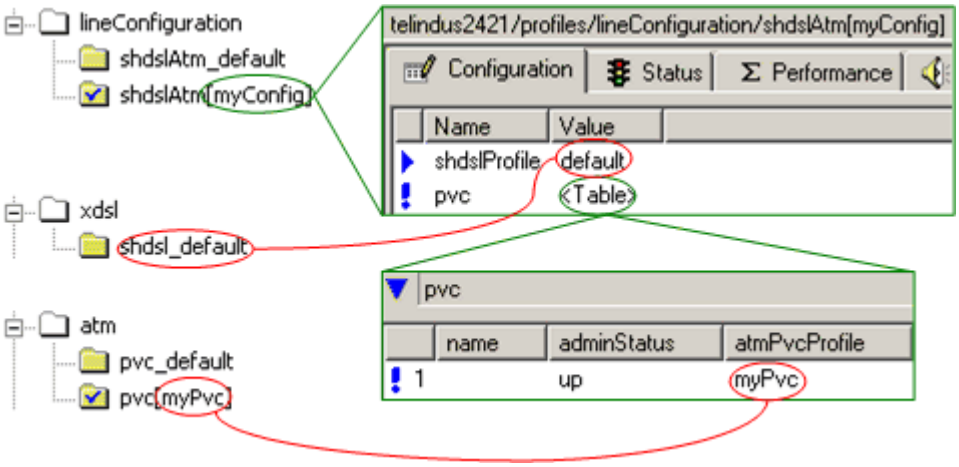
Example: applying an xDSL and ATM PVC profile on a line configuration profile

Suppose you have …

- a custom line configuration profile (profiles/lineConfiguration/shdslAtm[myConfig])
- a default xDSL profile (profiles/xdsl/shdsl_default)
- a custom ATM PVC profile (profiles/atm/pvc[myPvc])

… and want to apply the default xDSL profile and the custom ATM PVC profile on the custom line configuration profile.

In that case configure the shdslProfile attribute and the pvc/atmPvcProfile element in the custom line configuration profile as follows:

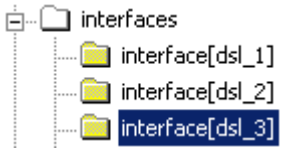
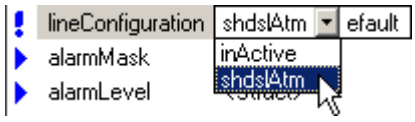
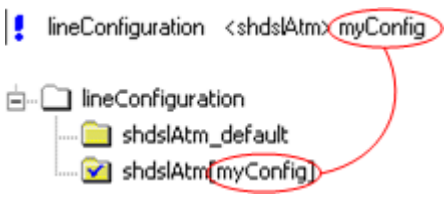


5.2.5 How to apply the line configuration profile?

Refer to 5.2 - How to create a configuration using profiles? on page 74 for an overview on how to create a configuration. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create an xDSL, ATM PVC and forwarding profile.
- Apply the forwarding profile on the ATM PVC profile.
- Create a line configuration profile.
- Apply the xDSL and ATM PVC profiles on the line configuration profile.
- → **Apply the line configuration profile on an xDSL line.** ← **You are here.**

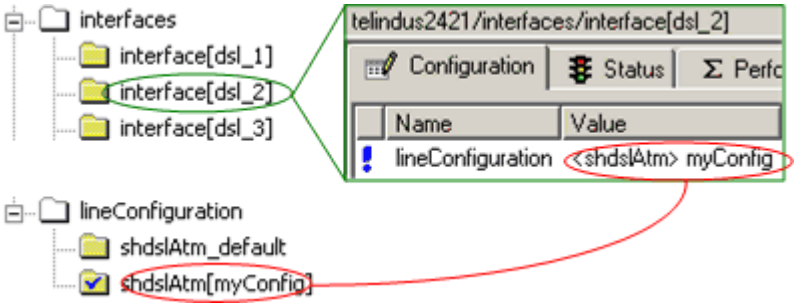
In order to apply the line configuration profile on an xDSL line, proceed as follows:

Step	Action
1	Go to an xDSL line object. E.g. to SHDSL line 3, i.e. dslInterfaces/interface[dsl_3]. 
2	Go to the attribute lineConfiguration.
3	First select the type of configuration you want to apply. Do this by using the first part of the value field. If you want … • that the xDSL line is not active, then select inActive. • to apply a line configuration profile, then select xdslAtm (where xdsl can be shdsl or adsl). 
4	Then type the name of the line configuration profile you want to apply. Do this in the second part of the value field. If you want to apply … • a default line configuration profile, then type the string “default”. • a custom line configuration profile, then type the index name of the custom line configuration object you previously added (refer to 5.2.3 - How to create a line configuration profile? on page 79). E.g. type the string “myConfig” if the custom line configuration object that you added is called profiles/lineConfiguration/shdslAtm[myConfig]. 

Example: applying a line configuration profile on an xDSL line

Suppose you have a custom line configuration profile (profiles/lineConfiguration/shdslAtm[myConfig]) and you want to apply this profile on xDSL line 2.

In that case configure the lineConfiguration attribute in the xDSL line object as follows:



6 Basic configuration

This chapter shows you how to configure the very basics of the Telindus 2400. Since this and the following chapters talk a lot about various interfaces, this chapter starts with describing what is meant by the term “interface”. Then this chapter shows you how to configure IP addresses on the different interfaces and how to configure passwords to control the management access to the Telindus 2400. Furthermore, there is a section on configuration actions, i.e. how to activate a configuration, how to load the default configuration, etc. The last section briefly explains what to check should you experience trouble when installing, configuring or operating the Telindus 2400.

The following gives an overview of this chapter:

- 6.1 - What is an interface? on page 86
- 6.2 - Configuring IP addresses on page 87
- 6.3 - Configuring the SHDSL line on page 97
- 6.4 - Configuring the ADSL line on page 104
- 6.5 - Configuring passwords on page 107
- 6.6 - Executing configuration actions on page 110
- 6.7 - Troubleshooting the Telindus 2400 on page 114

Refer to the Reference manual on page 295 for a complete overview of all the attributes of the Telindus 2400.

6.1 What is an interface?

The term interface, as it is used in this manual, can be divided into two groups:

Interface type	Description
physical	A physical interface is an interface to which you can physically connect a cable. So a physical interface has a physical connector. It also has some configuration attributes that control the behaviour of the interface. For example: • The control interface (CTRL). It has a female 9-pins subD connector to which you can connect a male 9-pins subD connector for maintenance purposes. It has configuration attributes such as ctrlPortProtocol, cms2Address, etc. • The LAN interface (LAN). It has a female RJ45 connector to which you can connect a male RJ45 connector to connect to an Ethernet network. It has configuration attributes such as ip, vlan, etc. Other examples are the station clock interface, the alarm interfaces, the xDSL line interfaces, etc.
logical	A logical interface is an interface to which you can not physically connect a cable. So a logical interface has no physical connector. However, it is part of the physical interface, but on a higher level. One physical interface can “contain” several logical interfaces. A logical interface also has some configuration attributes that control the behaviour of the interface. For example: • An ATM PVC on an xDSL line. The xDSL line is the physical interface (it has a physical connector) whereas the ATM PVC is the logical interface (it is located on a higher level, i.e. layer 2 protocol level). You can have several ATM PVCs on one xDSL line. • a VLAN on the LAN interface. The LAN interface is the physical interface and the VLAN is the logical interface. Other examples are L2TP tunnels, links in a multi-link bundle, bridge groups, etc.

6.2 Configuring IP addresses

The first thing you have to configure are the IP addresses of the Telindus 2400. First this section lists which mechanisms there are to obtain an IP address automatically. Then it shows you, for each interface, where you can find the IP related parameters. Finally this section explains these IP related parameters.

The following gives an overview of this section:

- 6.2.1 - Automatically obtaining an IP address on page 88
- 6.2.2 - Where to find the IP parameters? on page 89
- 6.2.3 - Explaining the ip structure on page 90
- 6.2.4 - Configuring an IP address on the LAN interface on page 95

6.2.1 Automatically obtaining an IP address

Obtaining an IP address on the LAN interface

The Telindus 2400 supports the BootP protocol to automatically obtain an IP address on its LAN interface.

Refer to 18 - Auto installing the Telindus 2400 on page 667 for more information on auto-install.

Obtaining IP addresses on the WAN interface

In case of …

- ATM, refer to 7.1.2 - Automatically obtaining IP addresses in ATM on page 123.
- PPP (in case of PPPoA), refer to 7.2.2 - Automatically obtaining IP addresses in PPP on page 141.

An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.

6.2.2 Where to find the IP parameters?

The following table shows where you can find the IP parameters of the different IP interfaces:

Interface	Location of the IP parameters
LAN interface	In the ip structure of the lanInterface object: telindus24xx/lanInterface/ip. **Important remark** If the configuration attribute telindus24xx/lanInterface/mode is set to bridging (default setting!), then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. So in this particular case, if you want to manage the Telindus 2400 via IP, then you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.
4 port Ethernet interface	In the ip structure of the 4pEth object: telindus24xx/4pEth/ip.
VLAN on the LAN interface	In the ip structure of the vlan table which is located in the lanInterface object: telindus24xx/lanInterface/vlan/ip.
VLAN on the 4 port Ethernet interface	In the ip structure of the vlan table which is located in the 4pEth object: telindus24xx/4pEth/vlan/ip.
ATM PVC on the xDSL lines	In the ip structure of the routing forwarding profile: telindus24xx/profiles/forwardingMode/routing_default/ip. By applying this profile on the ATM PVC profile, the IP parameters of the ATM PVC are configured. Refer to 7.1.3 - Configuring IP addresses in ATM on page 124.
ATM PVC on the 6E1 interface	In the ip structure of the pvc table which is located in the imaGroup object: telindus24xx/bundle/imaGroup[ ]/pvc/ip.
ATM PVC on the E3/T3 interface	In the ip structure of the pvc table which is located in the e3T3[E3T3_x]/atm object: telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/ip.
L2TP tunnel	In the ip structure of the l2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/l2tpTunnels/ip.
IPSEC L2TP tunnel	In the ip structure of the ipsecL2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/ip.
bridge group	In the ip structure of the bridgeGroup object: telindus24xx/bridge/bridgeGroup/ip.
management loopback	In the ipAddress attribute of the loopback object: telindus24xx/management/loopback/ipAddress.

Refer to 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.

6.2.3 Explaining the ip structure

Because the ip structure occurs in several objects, it is described here once and referenced where necessary. Refer to 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure.

This section lists all the elements that can be present in the ip structure. However, depending on the interface, it is possible that not all of these elements are present.

The ip structure contains the following elements:

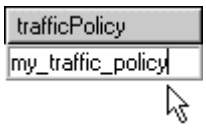
Element	Description
address	Use this element to assign an IP address to the interface. The address should belong to the subnet the interface is connected to. Default:0.0.0.0 Range: up to 255.255.255.255 If you do not explicitly configure a local IP address using the address element, then it can be learned. Refer to 6.2.1 - Automatically obtaining an IP address on page 88. An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.
netMask	Use this element to assign an IP subnet mask to the interface. The subnet mask defines the number of IP devices that may be present on the corresponding IP segment. Default:255.255.255.0 Range: up to 255.255.255.255
secondaryIp	Use this element to create additional virtual networks on the same Ethernet interface. Default:<empty> Range: table, see below The secondaryIp table contains the elements address and netMask. See above for an explanation of these elements.
remote	Use this element to assign an IP address to the remote end of an ATM PVC or an L2TP tunnel. Default:0.0.0.0 Range: up to 255.255.255.255 If you do not explicitly configure a remote IP address using the remote element, then it can be learned. Refer to 6.2.1 - Automatically obtaining an IP address on page 88. An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.

Element	Description
addrPool	Use this element to let the Telindus 2400 pick IP addresses out of an IP address pool (refer to What is an IP address pool?) and use these IP addresses as local and/or remote IP address of an ATM PVC. You can pick an IP address either out of … Default:<empty> Range: <choice, see below> • a list. First, select the string "list" using the first part of the addrPool value. Then, using the second part of the addrPool value, type the name of the list you previously created in the addrPools table. Refer to telindus24xx/ip/router/addrPools on page 419. addrPool <list> myList or • an interval. First, select the string "interval" using the first part of the addrPool value. Then, using the second part of the addrPool value, type the name of the interval you previously created in the addrPools table. Refer to telindus24xx/ip/router/addrPools on page 419. addrPool <interval> myInterval **What is an IP address pool?** An IP address pool is a collection of IP addresses from which the Telindus 2400 can pick an IP address and assign it to an interface. There are two types of IP pools: • an IP list pool. You create a list of IP addresses by entering them in a table. The Telindus 2400 picks a local and remote IP address out of this table. You can create an IP list pool using the configuration attribute addrPools. Refer to telindus24xx/ip/router/addrPools on page 419. Note again than an IP list pool is for *both local and remote IP addresses*. • an IP interval pool. You define a range of IP addresses. The Telindus 2400 picks a remote IP address out of this range. You can create an IP interval pool using the configuration attribute addrPools. Refer to telindus24xx/ip/router/addrPools on page 419. Note again that an IP interval pool is for *remote IP addresses only*. If you do not explicitly configure a local and/or remote IP address using the addrPool element, then it can be learned. Refer to 6.2.1 - Automatically obtaining an IP address on page 88. An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.
unnumbered	In case you do not explicitly configure a local IP address for an ATM PVC using the addrPool element, then you can use the unnumbered element to "borrow" the IP address of another interface for which an IP address is already configured, thereby conserving network and address space. Default:<empty> Range: 0 … 24 characters Do this by entering the interface name as unnumbered element value. unnumbered lan

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>acceptLocAddr</td><td>In case of a PPP(oA) link, it is possible to learn the local IP address from the remote side. Use the acceptLocAddr element to determine whether to accept or reject the learned IP address:
Default:enabled
Range: enabled / disabled
<table><tr><th>Value</th><th>Description</th></tr><tr><td>enabled</td><td>If the remote side is able to give an IP address, then the local IP address is learned from the remote side. Even if you explicitly configure a local IP address (e.g. using the address, addrPool or unnumbered element). In other words, if the acceptLocAddr element is set to enabled, then the local IP address that has been configured is overruled by the one that has been learned.</td></tr><tr><td>disabled</td><td>The local IP address can not be learned from the remote side.</td></tr></table>Also see 7.2.2 - Automatically obtaining IP addresses in PPP on page 141.

An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.</td></tr>
<tr><td>acceptRemAddr</td><td>In case of a PPP(oA) link, it is possible to learn the remote IP address from the remote side. Use the acceptRemAddr element to determine whether to accept or reject the learned IP address:
Default:enabled
Range: enabled / disabled
<table><tr><th>Value</th><th>Description</th></tr><tr><td>enabled</td><td>If the remote side is able to give an IP address, then the remote IP address is learned from the remote side. Even if you explicitly configure a local IP address (e.g. using the remote or addrPool element). In other words, if the acceptRemAddr element is set to enabled, then the remote IP address that has been configured is overruled by the one that has been learned.</td></tr><tr><td>disabled</td><td>The remote IP address can not be learned from the remote side.</td></tr></table>Also see 7.2.2 - Automatically obtaining IP addresses in PPP on page 141.

An IP address that is obtained using a dynamic procedure is not displayed in the configuration window, but can be found in the status window.</td></tr>
<tr><td>gatewayPreference</td><td>In case of a PPP(oA) link, if the remote IP address is learned from the remote side, then this route is automatically installed as default route to the remote. In that case you can use the gatewayPreference element to set the preference of this default route. Refer to the element preference on page 403 for more information.
Default:80
Range: 0 ... 90
Note that if you set the gatewayPreference element to 0, then the route is not installed.</td></tr>
</table>

Element	Description
rip	Use this element to configure the RIP related parameters of the interface. Default:- Range: structure, see below Refer to 9.5.3 - Explaining the rip structure on page 186 for a detailed description of the rip structure.
trafficPolicy	Use this element to apply a traffic policy on the routed data on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the traffic policy you want to use. You can create the traffic policy itself by adding an ipTrafficPolicy object under the profiles/policy/traffic object and by configuring the attributes in this object. **Example** If you created an ipTrafficPolicy object with index name my_traffic_policy (i.e. ipTrafficPolicy[my_traffic_policy]) and you want to apply this traffic policy here, then enter the index name as value for the trafficPolicy element.  Refer to 9.7 - Configuring traffic and priority policy on the router on page 207 for more information on policies. On the LAN interface, you can not apply a traffic policy with the purpose of queueing. On this interface, the traffic policy is intended to serve as extended access list. Refer to 12.2 - Configuring an extended access list on page 271.
directedBroadcasts	Use this element to enable (forward) or disable (discard) directed broadcasts. Default:enabled Range: enabled / disabled **What is a directed broadcast?** A directed broadcast is an IP packet destined for a complete (sub-)network. For example, a packet destined for all devices on subnetwork 192.168.48.0 with subnet mask 255.255.255.0 has destination address 192.168.48.255. I.e. all ones in the subnet area of the IP address.
icmpRedirects	Use this element to enable or disable the transmission of ICMP messages. Default:enabled Range: enabled / disabled **What is an ICMP redirect?** If icmpRedirects is enabled and if the Telindus 2400 receives an IP packet on the interface for which … • the next hop gateway is on the same interface, • the next hop address is in the same subnet as the source, … then it sends an ICMP message to the originator of the packet to inform him that a better (shorter) route exists.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>igmp</td><td>Use this element to configure the multicasting IGMP protocol.
Default:disabled
Range: enumerated, see below

The igmp element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Multicasts are not forwarded on this interface.</td></tr>
<tr><td>proxy</td><td>This is an upstream interface. It always serves as a client for the upstream router.

Multicasts are always forwarded on this interface.</td></tr>
<tr><td>router</td><td>This is a downstream interface. It serves as an IGMP querier or non-querier depending on the IP address.

Multicasts are forwarded on this interface if they are present in the upstream-interface multicast-member list.</td></tr>
</table>

Refer to What is IGMP? and IGMP topology on page 548 for more information on IGMP.</td></tr>
<tr><td>helpers</td><td>Use this element to enable broadcast forwarding.
Default:<empty>
Range: table, see below

Limited IP broadcasts (address 255.255.255.255) and (sub-)network broadcasts for a directly connected network are normally not forwarded by the Telindus 2400. However, client / server applications often use these broadcasts during start-up to discover the server on the network. If the server is on a remote LAN, then the detection may fail.

Therefore, if you configure a helper IP address, the received broadcasts address is replaced by this helper IP address and the packets are re-routed using the destination address. Multiple helper IP addresses can be configured.

The Telindus 2400 only substitutes addresses for the protocols which are selected in the helperProtocols attribute. Refer to telindus24xx/ip/router/helperProtocols on page 409.</td></tr>
<tr><td>nat</td><td>Use this element to enable address translation on the interface.
Default:<empty>
Range: 0 … 24 characters

Do this by entering the string “default“ as nat element value. By doing so, the settings are applied as defined in the router/defaultNat object. In future releases, it will also be possible to refer to a user defined NAT object (analogous to the routing filter, traffic policy, etc.).

Refer to …

• 9.6 - Configuring address translation on page 191 for more information on NAT.
• 13.12.2 - Default NAT configuration attributes on page 426 for a detailed description of the NAT configuration attributes.</td></tr>
</table>

6.2.4 Configuring an IP address on the LAN interface

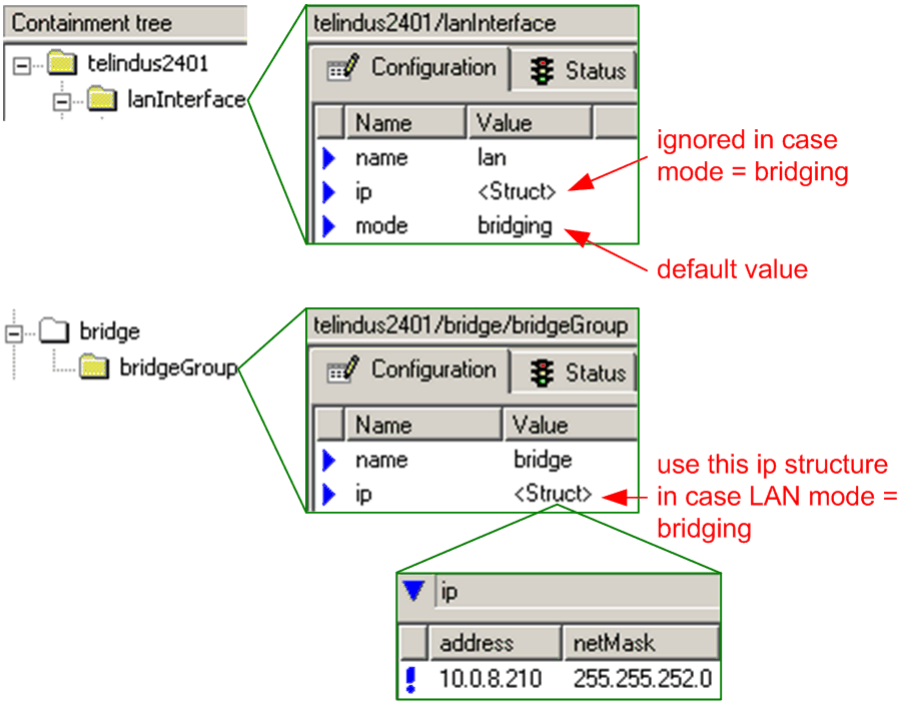
When configuring an IP address on the LAN interface, there are two different scenarios:

- The LAN interface mode is *bridging* (the configuration attribute telindus24xx/lanInterface/mode is set to bridging). This is the default setting.
- The LAN interface mode is *routing* (the configuration attribute telindus24xx/lanInterface/mode is set to routing).

LAN interface mode = bridging

In this case the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. If you want to manage the Telindus 2400 via IP, then you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.

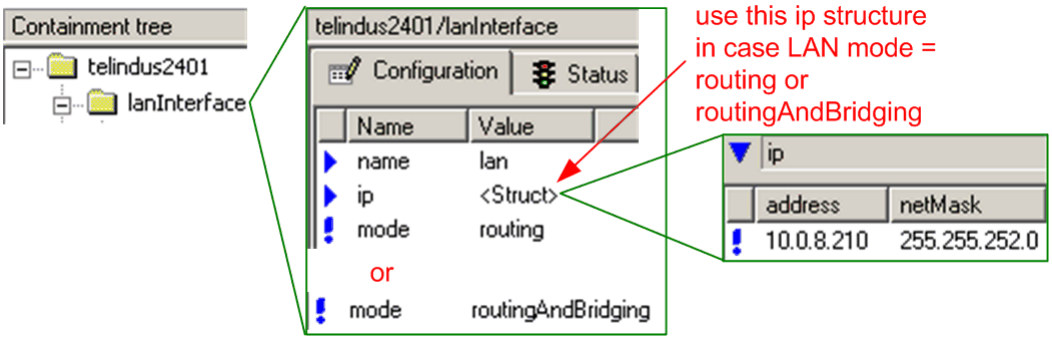
Suppose you want to assign IP address 10.0.8.210 with subnet mask 255.255.252.0 to the LAN interface, then configure the appropriate attributes as follows:



LAN interface mode = routing

In this case the settings of the configuration attribute telindus24xx/lanInterface/ip are used.

Suppose you want to assign IP address 10.0.8.210 with subnet mask 255.255.252.0 to the LAN interface, then configure the appropriate attributes as follows:



6.3 Configuring the SHDSL line

This section applies on the Telindus 2400 SHDSL models only (2421, 2422, 2423).

If you want to establish a connection over an SHDSL line, then you have to set up the necessary profiles (refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63). This section gives an overview of the basic configuration attributes that are present in an SHDSL profile. Furthermore, this section also lists which SHDSL line configuration attributes are set to a fixed value (i.e. they are not configurable).

The following gives an overview of this section:

- 6.3.1 - Basic SHDSL line configuration attributes on page 98
- 6.3.2 - Selecting an SHDSL line speed (range) on page 99
- 6.3.3 - Creating a dual pair SHDSL line on page 100
- 6.3.4 - Fixed SHDSL line attributes on page 101
- 6.3.5 - Compatibility with other SHDSL devices on page 103

6.3.1 Basic SHDSL line configuration attributes

In order to successfully establish connection over an SHDSL line, it is essential that the following configuration attributes are configured correctly:

Attribute	Purpose of the attribute
telindus24xx/profiles/xdsl/shdsl_default/region on page 356	Use this attribute to select the correct SHDSL standard.
telindus24xx/profiles/xdsl/shdsl_default/mode on page 356	Use this attribute to select 1 pair or 2 pair operation. This is important if the remote SHDSL device is a 1 pair or 2 pair device. Refer to 6.3.3 - Creating a dual pair SHDSL line on page 100 for more information on selecting 1 pair or 2 pair operation.
If you configured an SHDSL line for 1 pair operation, then use: • telindus24xx/profiles/xdsl/shdsl_default/minSpeed on page 357 • telindus24xx/profiles/xdsl/shdsl_default/maxSpeed on page 357 If you configured an SHDSL line for 2 pair operation, then use: • telindus24xx/profiles/xdsl/shdsl_default/minSpeed2P on page 357 • telindus24xx/profiles/xdsl/shdsl_default/maxSpeed2P on page 357	Use these attributes to select an appropriate speed (range) for a successful and qualitative line connection. Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information on the speed (range).

Refer to 13.10.1 - SHDSL profile configuration attributes on page 355 for a complete overview of the SHDSL line configuration attributes.

6.3.2 Selecting an SHDSL line speed (range)

Selecting a speed range

The Telindus 2400 features auto speed negotiation according to ITU-T G.994.1. During this negotiation the Telindus 2400 selects a speed within the range from the minimum speed up to the maximum speed as set with the minSpeed(2P) and maxSpeed(2P) attributes.

Important remark

If you configured an SHDSL line for 2 pair operation then define a speed range *either* on the Telindus 2400 *or* on the remote SHDSL device, *but not on both*. Else the 2 line pairs could train at a different speed which is not allowed.

Selecting a fixed speed

If you set the minSpeed(2P) and maxSpeed(2P) attribute to the same value, then the Telindus 2400 operates at a fixed speed.

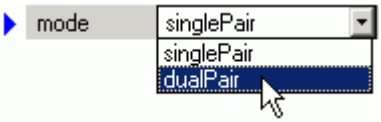
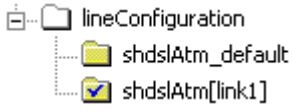
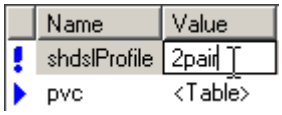
Fall-back speed

When you define a speed range, the Telindus 2400 will always try to operate at the maximum speed. If the remote does not allow that speed or the signal quality deteriorates, then the Telindus 2400 tries to select the second speed down the range. If also this speed fails, the Telindus 2400 again lowers its speed. It does this until it reaches the minimum speed.

6.3.3 Creating a dual pair SHDSL line

By default, a line only contains 1 line pair. However, you can create a line which contains 2 line pairs. Do this by creating a specific “2 pair” profile.

In order to create a 2 pair line, proceed as follows:

Step	Action
1	Under the profiles/xdsl object, add an shdsl[ ] object. Refer to 4.4 - Adding an object to the containment tree on page 56. E.g. shdsl[2pair]
2	Under the shdsl[ ] object you just added, set the attribute mode to dualPair. 
3	Create a line configuration profile. Refer to 5.2.3 - How to create a line configuration profile? on page 79. E.g. shdslAtm[link1] 
4	In the line configuration profile you created in step 3, apply the SHDSL profile you created in step 1. Do this by entering the index name of the SHDSL profile you created in step 1 in the attribute shdslProfile of the line configuration profile you created in step 3. 
5	Go to the object of the SHDSL line which you want to be taken as line pair 1 and apply the line configuration profile you created in step 3. Do this by entering the index name of the line configuration profile you created in step 3 in the attribute lineConfiguration of the SHDSL line object. E.g. lineConfiguration = <shdslAtm> link1 **Important remark** The first line pair of a dual pair line always has to be a line pair with an uneven index number. E.g. 1, 3, 5, 7, etc.
6	Activate the configuration by clicking the *Send all attributes to device* button . Before you can see the effect, first click on the *Reconnect* button . The result looks as follows:

6.3.4 Fixed SHDSL line attributes

As opposed to other Telindus SHDSL devices, on the Telindus 2400 some SHDSL line configuration attributes are set to a fixed value (i.e. they are not configurable). To be able to configure the other Telindus SHDSL devices so that they can operate with the Telindus 2400 it is useful to know which are these fixed attributes and to which value they are fixed. Therefore, this section describes the fixed line features of the Telindus 2400.

The following gives an overview of this section:

- Power back-off (always enabled) on page 101
- The channel attribute (fixed to central) on page 101
- The timingMode attribute (fixed to synchronous) on page 101
- The eocHandling attribute (fixed to alarmConfiguration) on page 102

Power back-off (always enabled)

The Telindus 2400 features power back-off. Power back-off is a part of the ITU-T G.991.2 SHDSL recommendation. It reduces the maximum transmit power level if the line conditions are sufficiently good to operate at a lower transmit level.

Power back-off is performed by default (no configuration attribute). During the ITU-T G.994.1 handshake, the two sides of the line mutually agree on the transmit level. The transmit level is lowered between 0 and 6 dB in steps of 1dB.

The channel attribute (fixed to central)

On a Telindus SHDSL device such as the Crocus SHDSL for instance, you can configure a line attribute called channel. This attribute determines which device acts as master and which as slave during the training sequence of the line. You can set the channel attribute to central or remote.

On the Telindus 2400 you can not configure the channel attribute (it is even not present in the containment tree). It is fixed to the value central. This implies that on any Telindus SHDSL device that you connect to the Telindus 2400, the channel attribute has to be set to remote.

The timingMode attribute (fixed to synchronous)

On a Telindus SHDSL device such as the Crocus SHDSL for instance, you can configure a line attribute called timingMode. This attribute determines how the user interface clock is coupled with the line clock.

On the Telindus 2400 you can not configure the timingMode attribute (it is even not present in the containment tree). It is fixed to the value synchronous. This implies that on any Telindus SHDSL device that you connect to the Telindus 2400, the timingMode attribute also has to be set to synchronous.

The eocHandling attribute (fixed to alarmConfiguration)

On a Telindus SHDSL device such as the Crocus SHDSL for instance, you can configure a line attribute called eocHandling. This attribute determines the handling of the EOC messages.

On the Telindus 2400 you can not configure the eocHandling attribute (it is even not present in the containment tree). It is fixed to the value alarmConfiguration.

What is EOC?

SHDSL devices can communicate with each other through the Embedded Operations Channel (EOC). For instance the Telindus 2400 can send the following types of EOC requests:

- inventory, to get information (manufacturer, release, etc.) about the remote SHDSL device,
- enable / disable network loop-backs on the remote SHDSL device,
- ask the CPE to report statistics or failure information (SNR Margin, loop attenuation, number of CRC errors, etc.).

The EOC messages are defined in G.991.2 to provide interoperability.

How does the Telindus 2400 handle EOC?

The Telindus 2400 “scans” the SHDSL line. For every device it discovers, it adds an object to the containment tree. Refer to Discovering devices on the SHDSL line.

Then the Telindus 2400 retrieves information from these devices and displays it in the corresponding objects. Additionally, the Telindus 2400 device forces the remote SHDSL device to use the link alarm thresholds lineAttenuationOn and noiseMarginOn as configured on the Telindus 2400 itself. In other words, the settings of the lineAttenuationOn and noiseMarginOn on the Telindus 2400 overrule those of the remote SHDSL device.

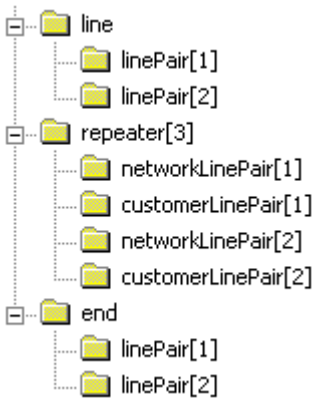
Discovering devices on the SHDSL line

The Telindus 2400 “scans” the line in order to determine which devices are present between itself and its remote counterpart.

When the scan is finished, some new objects are added to the containment tree[1] on the same level as the line object:

- If one or more repeaters are present on the SHDSL line, a repeater[ ] object is added for every repeater.
- For the remote counterpart, an end object is added.

For example, suppose you have a link with a Telindus 2400 as central device, a Crocus SHDSL as remote device and one Crocus SHDSL Repeater in between. In that case one repeater[ ] object and an end object is added to the containment tree as can be seen in the figure.



1. It can take up to 5 minutes before the new objects appear in the containment tree.

6.3.5 Compatibility with other SHDSL devices

The Telindus 2400 can be used in combination with other (Telindus) SHDSL devices. The interoperability for Telindus SHDSL products document (PDF) gives an overview of the interoperability.

6.4 Configuring the ADSL line

This section applies on the Telindus 2400 ADSL models only (2401, 2402, 2403).

If you want to establish a connection over an ADSL line, then you have to set up the necessary profiles (refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63). This section gives an overview of the basic configuration attributes that are present in an ADSL profile.

The following gives an overview of this section:

- 6.4.1 - Basic ADSL line configuration attributes on page 105
- 6.4.2 - Selecting an ADSL line speed (range) on page 106

6.4.1 Basic ADSL line configuration attributes

In order to successfully establish connection over an ADSL line, it is essential that the following configuration attributes are configured correctly:

Attribute	Purpose of the attribute
telindus24xx/profiles/xdsl/adsl_default/standard on page 363	Use this attribute to select the correct ADSL standard.
For the upstream data, use: • telindus24xx/profiles/xdsl/adsl_default/usMinSpeed on page 364 • telindus24xx/profiles/xdsl/adsl_default/usMaxSpeed on page 364 For the downstream data, use: • telindus24xx/profiles/xdsl/adsl_default/dsMinSpeed on page 364 • telindus24xx/profiles/xdsl/adsl_default/dsMaxSpeed on page 364	Use these attributes to select an appropriate speed (range) for a successful and qualitative line connection. Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information on the speed (range).
telindus24xx/profiles/xdsl/adsl_default/latency on page 365	Use this attribute to configure the latency of the ADSL line.

Refer to 13.10.2 - ADSL profile configuration attributes on page 362 for a complete overview of the ADSL line configuration attributes.

6.4.2 Selecting an ADSL line speed (range)

Selecting a speed range

The Telindus 2400 features auto speed negotiation. During this negotiation the Telindus 2400 selects a speed within the range from the minimum speed up to the maximum speed as set with the usMinSpeed / dsMinSpeed and usMaxSpeed / dsMaxSpeed attributes.

Selecting a fixed speed

If you set the minSpeed and maxSpeed attributes to the same value, then the Telindus 2400 operates at a fixed speed.

Fall-back speed

When you define a speed range, the Telindus 2400 will always try to operate at the maximum speed. If the remote does not allow that speed or the signal quality deteriorates, then the Telindus 2400 tries to select the second speed down the range. If also this speed fails, the Telindus 2400 again lowers its speed. It does this until it reaches the minimum speed.

Speed versus ADSL standard

Note that the different ADSL standards support different speed ranges (refer to telindus24xx/profiles/xdsl/adsl_default/standard on page 363).

6.5 Configuring passwords

This section shows you how to create a (list of) password(s) with associated access level in the security table. It also explains how to correct the security table in case of error or in case you forgot your password. Furthermore, this section shows you how to enter the passwords in the different maintenance tools.

The following gives an overview of this section:

- 6.5.1 - Adding passwords to the security table on page 108
- 6.5.2 - Correcting the security table on page 108
- 6.5.3 - Entering passwords in the different management tools on page 109

6.5.1 Adding passwords to the security table

In order to avoid unauthorised access to the Telindus 2400 and the network you can create a list of passwords with associated access levels in the security table. Do this using the security attribute. Refer to telindus24xx/security on page 308.

6.5.2 Correcting the security table

If you forgot your password or you forgot to create one with write and security access, then you can set the *Load Default Configuration* DIP switch. As a result, the Telindus 2400 reboots in its default configuration. You can then retrieve the erroneous configuration and correct it.

To correct the security table, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 40.
2	Set DIP switch bank DS1 position 2 to *off*. Refer to 3.1 - The Telindus 2400 motherboard on page 38 to locate this DIP switch bank.
3	Slide the bottom in the cover again without fastening the screws and reconnect the power supply. ⇒The Telindus 2400 reboots and loads the default configuration.
4	Retrieve the erroneous configuration: **Step** / **Action** 1 — Open a TMA session on the Telindus 2400. Refer to 4.1 - Maintaining the Telindus 2400 with TMA on page 42. 2 — Execute the Load Saved Configuration action. 3 — Change the password and/or access rights in the security table. 4 — Execute the Activate Configuration action.
5	Again, disconnect the power supply and open the housing.
6	Reset DIP switch bank DS1 position 2 to *on*.
7	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 40 and reconnect the power supply.

6.5.3 Entering passwords in the different management tools

Now that you created a (list of) password(s) in the Telindus 2400, you have to enter these passwords every time you want to access the Telindus 2400 with one of the maintenance or management tools.

The following table explains how to enter passwords in the different maintenance or management tools:

Maintenance or management tool	**How to enter the password?**
TMA	Enter the password in the *Connect…* window.
TMA CLI, TMA Element Management and TMA for HP OpenView	Use the application *TmaUserConf.exe* to create a TMA user and assign a password to this user. The password should correspond with a password configured in the device. Refer to the manual of TMA CLI (PDF), TMA Element Management (PDF/CHM) or TMA for HP OpenView (PDF) for more information.
CLI	You are prompted to enter the password when the session starts.
ATWIN	You are prompted to enter the password when the CLI session starts. Then you can start an ATWIN session.
Web Interface	You are prompted to enter the password when the session starts.
SNMP	Define the password as community string. If no passwords are defined, then you can use any string as community string.
TML	Enter the password after the destination file name. Separate password and file name by a '?'. Example: `tml -fsourcefile@destinationfile?pwd`
(T)FTP	Enter the password after the destination file name. Separate password and file name by a '?'. Example: `put sourcefile destinationfile?pwd`

6.6 Executing configuration actions

This section shows you how to execute actions on the configuration. The following gives an overview of this section:

- 6.6.1 - What are the different configuration types? on page 111
- 6.6.2 - Activating the configuration on page 112
- 6.6.3 - Loading the default configuration on page 112
- 6.6.4 - Loading the default configuration using a DIP switch on page 113

6.6.1 What are the different configuration types?

This section explains the different configuration types that are present in the Telindus 2400.

Which are the configuration types?

Three types of configuration are present in the Telindus 2400:

- the non-active configuration
- the active configuration
- the default configuration.

Explaining the configuration types

When you configure the Telindus 2400, the following happens:

Phase	Action	Result
1	Connect the computer running the maintenance tool to the Telindus 2400.	The non-active configuration is displayed on the screen.
2	Modify the non-active configuration.	The modifications have no immediate influence on the active configuration currently used by the Telindus 2400.
3	Complete the modifications on the non-active configuration.	The non-active configuration has to be activated.
4	In case of … • TMA, click on the TMA button *Send all attributes to device*: . • any other maintenance tool than the graphical user interface based TMA (e.g. ATWIN, CLI, Web Interface, EasyConnect terminal, TMA CLI), then execute the Activate Configuration action.	The non-active configuration becomes the active configuration.

Which are the configuration actions?

You can execute the following actions on the configuration:

- telindus24xx/Activate Configuration on page 310
- telindus24xx/Load Default Configuration on page 310
- telindus24xx/Load Saved Configuration on page 311

6.6.2 Activating the configuration

As explained in section 6.6.1 - What are the different configuration types? on page 111, when you finished configuring the Telindus 2400 you have to activate the configuration changes you made.

In case of …

- TMA, click on the TMA button *Send all attributes to device*: .
- any other maintenance tool than the graphical user interface based TMA (e.g. ATWIN, CLI, Web Interface, EasyConnect terminal, TMA CLI), then execute the Activate Configuration action.

6.6.3 Loading the default configuration

If you install the Telindus 2400 for the first time, all configuration attributes have their default values. If the Telindus 2400 has already been configured but you want to start from scratch, then you can revert to the default configuration.

You can load the default configuration using the *Load Default Configuration* …

- action. Refer to telindus24xx/Load Default Configuration on page 310.
- DIP switch. Refer to 6.6.4 - Loading the default configuration using a DIP switch on page 113.

6.6.4 Loading the default configuration using a DIP switch

The following procedure shows how to load the default configuration using the *Load Default Configuration* DIP switch on the Telindus 2400 PCB:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 40.
2	Set DIP switch bank DS1 position 2 to *off*. Refer to 3.1 - The Telindus 2400 motherboard on page 38 to locate this DIP switch bank.
3	Slide the bottom in the cover again without fastening the screws and reconnect the power supply. ⇒The Telindus 2400 reboots and loads the default configuration.
4	Activate the loaded default configuration: <table><tr><th>Step</th><th>Action</th></tr><tr><td>1</td><td>Open a TMA session on the Telindus 2400. Refer to 4.1 - Maintaining the Telindus 2400 with TMA on page 42.</td></tr><tr><td>2</td><td>Execute the Activate Configuration action.[1]</td></tr></table> 1. If you are performing this load default configuration procedure because you accidentally made a configuration error, you have the possibility to retrieve this erroneous configuration before executing the Activate Configuration command. In that case you do not have to reconfigure the complete device again, but you only have to correct the error in question. Retrieve the erroneous configuration by executing the Load Saved Configuration command.
5	Again, disconnect the power supply and open the housing.
6	Reset DIP switch bank DS1 position 2 to *on*.
7	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 40 and reconnect the power supply.

6.7 Troubleshooting the Telindus 2400

If you experience trouble when installing, configuring or operating the Telindus 2400, then check the following:

Check	Description
power	Is the Telindus 2400 powered properly?
connections	Are all the necessary cables connected to the Telindus 2400? Are they connected to the correct connectors of the Telindus 2400? Are they connected properly? Did you use the correct cables (straight, crossed, …)? Refer to 2.6 - Connecting the Telindus 2400 on page 25.
other devices	Are the devices that are connected to the Telindus 2400 working properly (are they powered, are they operational, …)?
LEDs	What indicate the LEDs of the Telindus 2400? Do they indicate a fault condition? Refer to 2.7 - The front panel LED indicators on page 33.
messages	What messages are displayed in the messages table? This table displays informative and error messages. Refer to telindus24xx/messages on page 483.
status	What indicate the status attributes of the Telindus 2400? What is the status of the different interfaces (up, down, testing, …)? Refer to 14 - Status attributes on page 473.
performance	What indicate the performance attributes of the Telindus 2400? What is the performance of the different interfaces (does the data pass the interface, is the interface up or down, when did it go up or down, …)? Refer to 15 - Performance attributes on page 579.
alarms	What indicate the alarm attributes of the Telindus 2400? What is the alarm status of the different interfaces (link down, errors, …)? Refer to 16 - Alarm attributes on page 641.

7 Configuring the encapsulation on the xDSL lines

This chapter introduces the encapsulation protocols that you can use on the xDSL lines and lists the attributes you can use to configure the encapsulation protocols.

The following gives an overview of this chapter:

- 7.1 - Configuring ATM encapsulation on page 116
- 7.2 - Configuring PPP encapsulation (in case of PPPoA) on page 137

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

7.1 Configuring ATM encapsulation

This section introduces the ATM encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol.

The following gives an overview of this section:

- 7.1.1 - Introducing ATM on page 117
- 7.1.2 - Automatically obtaining IP addresses in ATM on page 123
- 7.1.3 - Configuring IP addresses in ATM on page 124
- 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126
- 7.1.5 - Configuring UBR on page 129
- 7.1.7 - ATM PVC bandwidth redistribution on page 131
- 7.1.8 - Configuring bridged/routed Ethernet/IP over ATM (RFC 2684) on page 134
- 7.1.9 - Configuring Classical IP (IPoA) on page 135
- 7.1.10 - Configuring PPP over ATM (PPPoA) on page 136

7.1.1 Introducing ATM

What is ATM?

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides scalable bandwidth. Because of its asynchronous nature, ATM is more efficient than synchronous technologies, such as time-division multiplexing (TDM).

With TDM, each user is assigned a time slot, and no other station can send in that time slot. If a station has much data to send, it can send only when its time slot comes up, even if all other time slots are empty. However, if a station has nothing to transmit when its time slot comes up, the time slot is sent empty and is wasted. Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell.

What is VPI and VCI?

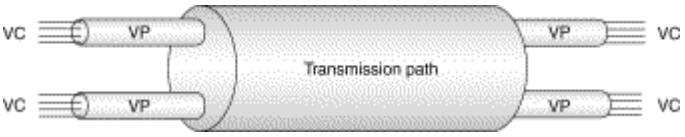
ATM networks are fundamentally connection-oriented, which means that a virtual channel must be set up across the ATM network prior to any data transfer. (A virtual channel is roughly equivalent to a Permanent Virtual Circuit or PVC.)

Two types of ATM connections exist:

- virtual paths, which are identified by Virtual Path Identifiers (VPIs).
- virtual channels, which are identified by the combination of a VPI and a Virtual Channel Identifier (VCI).

A virtual path is a bundle of virtual channels, all of which are switched transparently across the ATM network based on the common VPI. All VPIs and VCIs, however, have only local significance across a particular link and are remapped, as appropriate, at each switch.

A transmission path is the physical media that transports virtual channels and virtual paths. The following figure illustrates how VCs concatenate to create VPs, which, in turn, traverse the media or transmission path.



What are the ATM layers?

The ATM reference model is composed of the following ATM layers:

Layer	Description
physical layer	Analogous to the physical layer of the OSI reference model, the ATM physical layer manages the medium-dependent transmission.
ATM layer	Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model. The ATM layer is responsible for the simultaneous sharing of virtual circuits over a physical link (cell multiplexing) and passing cells through the ATM network (cell relay). To do this, it uses the VPI and VCI information in the header of each ATM cell.
ATM Adaptation Layer (AAL)	Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model. The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes. The adaptation layer prepares user data for conversion into cells and segments the data into 48-byte cell payloads. At present, the four types of AAL recommended by the ITU-T are AAL1, AAL2, AAL3/4, and AAL5:
higher layers	Finally, the higher layers residing above the AAL accept user data, arrange it into packets, and hand it to the AAL.

AAL	Description
AAL1	AAL1 is used for connection-oriented, delay-sensitive services requiring constant bit rates, such as uncompressed video and other isochronous traffic.
AAL2	AAL2 is used for connection-oriented services that support a variable bit rate, such as some isochronous video and voice traffic.
AAL3/4	AAL3/4 (merged from two initially distinct adaptation layers) supports both connectionless and connection-oriented links but is used primarily for the transmission of SMDS packets over ATM networks.
AAL5	AAL5 supports connection-oriented VBR services and is used predominantly for the transfer of classical IP over ATM and LANE traffic. AAL5 uses SEAL and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

What are ATM service categories?

The Traffic Management Specification Version 4.0 defines five ATM service categories that describe the traffic transmitted by users onto a network and the Quality of Service (QoS) that a network needs to provide for that traffic. The five service categories are:

- Constant Bit Rate (CBR)
- Variable Bit Rate non-real-time (VBR-nrt)
- Variable Bit Rate real-time (VBR-rt)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

The Telindus 2400 supports UBR .

What is UBR?

Unspecified Bit Rate (UBR) is an ATM bandwidth-allocation service that does not guarantee any throughput levels and uses only available bandwidth. UBR is intended for non-real-time applications that do not require any maximum bound on the transfer delay or on the cell loss ratio.

Advantages	• UBR allows for a high degree of statistical multiplexing by not reserving any minimum bandwidth per PVC. The PVCs use the bandwidth up to the configured PCR when available. • UBR models the best-effort service normally provided by the Internet. Suitable for applications tolerant to delay and not requiring real-time response. Examples include e-mail, fax transmission, file transfers, telnet, LAN and remote office interconnections. Such applications are not sensitive to delay, but they are sensitive to cell loss.
Disadvantages	UBR PVCs can experience a large number of cell drops or a high cell transfer delay as cells move from the source to the destination device.

The only traffic parameter you have to configure in case of UBR is the PCR. The PCR only provides an indication of a physical bandwidth limitation within a PVC.

What is multi-protocol over ATM (MPoA)?

As its name implies, multi-protocol encapsulation over ATM provides mechanisms for carrying traffic other than just IP. Several different protocols can be used on top of ATM:

- Bridged/routed Ethernet/IP over ATM (formerly RFC 1483, now RFC 2684). This protocol makes the router appear as a LAN device to the operating system.
- IP over ATM (IPoA, RFC 1577, similar to RFC 2684). Also in this case the protocol makes the router appear as a LAN device to the operating system.
- Point to Point Protocol Over ATM (PPPoA, RFC 2364). PPP provides session setup, user authentication (login), and encapsulation for upper layer protocols such as IP. The use of PPP makes the router appear as a dial device to the operating system.
- Point to Point Protocol Over Ethernet (PPPoE, RFC 2516). This protocol makes the router appear as a LAN device to the operating system. It allows multiple devices on an Ethernet to share a common connection to the remote network (e.g. the Internet).

Which are the multi-protocol over ATM encapsulation mechanisms?

As said before, you can encapsulate several protocols in ATM. The mechanisms to do this are:

MPoA encapsulation mechanism	Description
Logical Link Control (LLC) encapsulation	In this method, multiple protocol types can be carried across a single connection with the type of encapsulated packet identified by a standard LLC/SNAP header.
Virtual Connection Multiplexing	In this method, only a single protocol is carried across an ATM connection, with the type of protocol implicitly identified at connection setup.

LLC encapsulation is provided to support routed and bridged protocols. In this encapsulation format, PDUs from multiple protocols can be carried over the same virtual connection. The type of protocol is indicated in the packet's SNAP header. By contrast, the virtual connection multiplexing method allows for transport of just one protocol per virtual connection.

What is PPPoA (RFC 2364)?

PPP over ATM adaptation layer 5 (AAL5) uses AAL5 as the framed protocol. It relies on RFC 2684, operating in either Logical Link Control Encapsulation or Virtual Connection Multiplexing mode. A Customer Premises Equipment (CPE) device encapsulates the PPP session based on this RFC for transport across the xDSL loop and the Digital Subscriber Line Access Multiplexer (DSLAM).

What are OAM F4 loop-back cells?

The ATM protocol features OAM F4 loop-back cells. Whereas OAM F5 loop-back cells are used to verify whether a *Virtual Channel* is truly up or down, the OAM F4 loop-back cells are used to verify whether a *Virtual Path* is truly up or down.

What are OAM F5 loop-back cells?

The ATM protocol features OAM F5 loop-back cells. Whereas OAM F4 loop-back cells are used to verify whether a *Virtual Path* is truly up or down, the OAM F5 loop-back cells are used to verify whether a *Virtual Channel* is truly up or down.

What is CLP?

The Cell Loss Priority (CLP) indicates whether the cell should be discarded if it encounters extreme congestion as it moves through the network. If the CLP bit equals 1, the cell should be discarded in preference to cells with the CLP bit equal to 0.

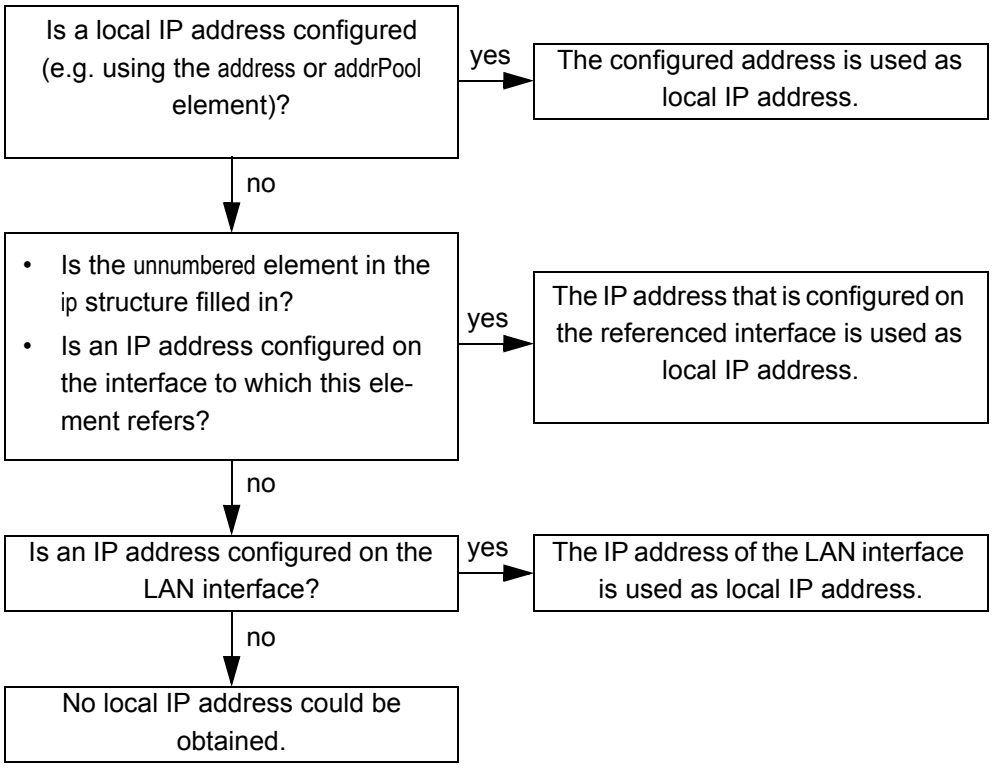
What is EFCI?

The Explicit Forward Congestion Indication (EFCI) indicates whether a cell containing user data experienced congestion as it moved through the network.

7.1.2 Automatically obtaining IP addresses in ATM

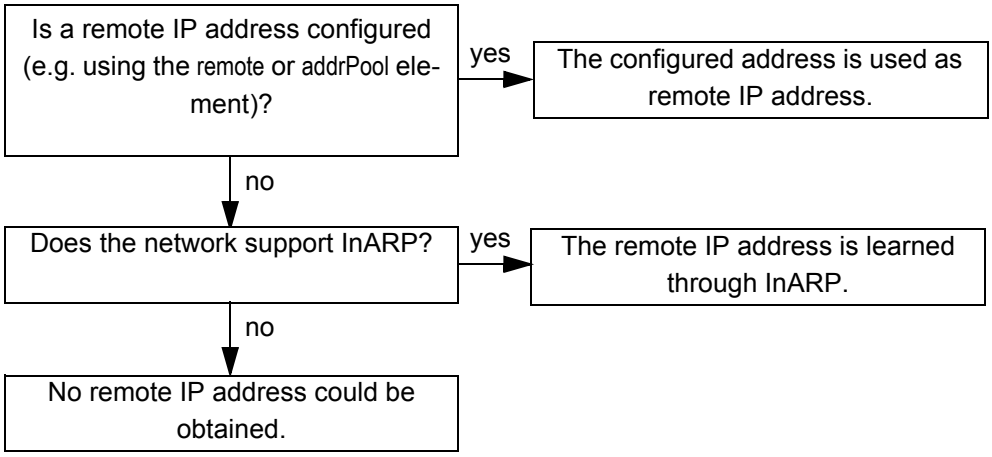
Obtaining a local IP address

In case of ATM, the Telindus 2400 currently does not support an automatic procedure to learn the local IP address of an ATM PVC. However, if you do not configure the local IP address (using either the addrPool or unnumbered element of the ip structure), then the IP address of the LAN interface is used.


Is a local IP address configured (e.g. using the address or addrPool element)?
yes
The configured address is used as local IP address.
no
• Is the unnumbered element in the ip structure filled in?
• Is an IP address configured on the interface to which this element refers?
yes
The IP address that is configured on the referenced interface is used as local IP address.
no
Is an IP address configured on the LAN interface?
yes
The IP address of the LAN interface is used as local IP address.
no
No local IP address could be obtained.

Obtaining a remote IP address

If the ATM network supports the InARP (Inverse Address Resolution Protocol) protocol, then the Telindus 2400 can learn the remote IP address of an ATM PVC.


Is a remote IP address configured (e.g. using the remote or addrPool element)?
yes
The configured address is used as remote IP address.
no
Does the network support InARP?
yes
The remote IP address is learned through InARP.
no
No remote IP address could be obtained.

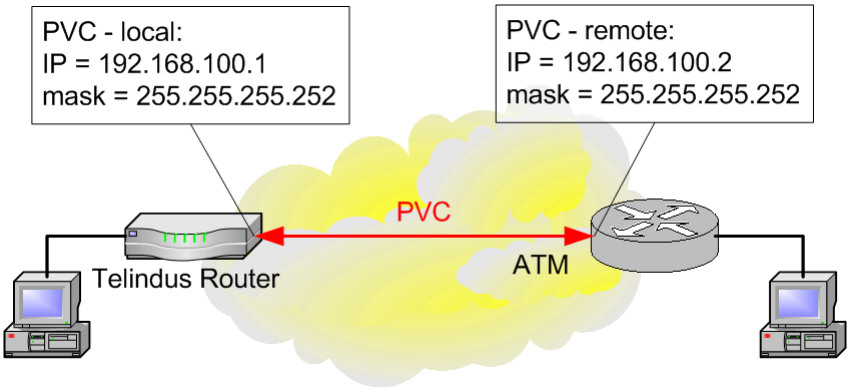
7.1.3 Configuring IP addresses in ATM

To configure IP addresses on an ATM PVC, proceed as follows:

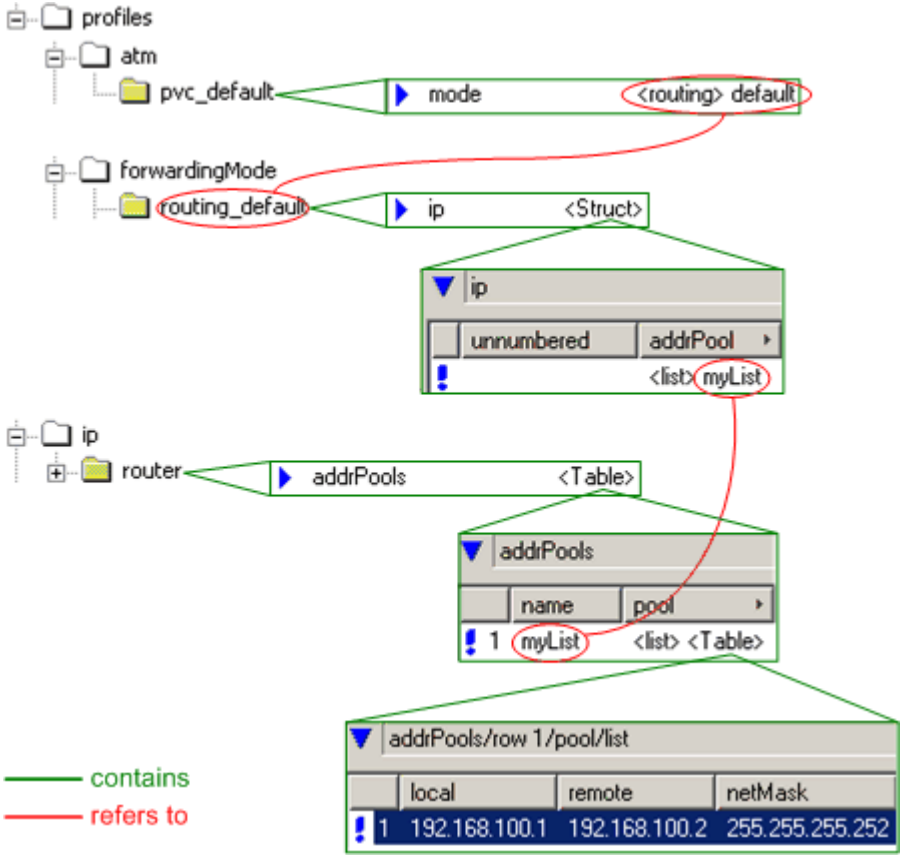
Step	Action
1	First create a routing forwarding profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
2	In the routing forwarding profile you just created, configure the ip structure. It is in this structure that you can configure the IP addresses (and other IP related attributes). The most important elements of the ip structure are: • unnumbered. Use this element to “borrow” an IP address from another interface. • addrPool. Use this element to pick an IP address out of an IP address pool. Refer to 6.2.3 - Explaining the ip structure on page 90.
3	Create an ATM PVC profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
4	Apply the routing forwarding profile on the ATM PVC profile. Refer to 5.2.2 - How to apply the forwarding profile? on page 77. ⇒By doing so, you configured the IP addresses of one ATM PVC. However, before this ATM PVC becomes active, you still have to add it to the PVC table and apply it on an xDSL line. Refer to 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126.

Example - configuring IP addresses on an ATM PVC

The following figure shows a set-up where two LAN networks are connected to each other over an ATM PVC.



The following figure shows how to configure the IP addresses on the ATM PVC.



7.1.4 Configuring ATM PVCs - the ATM PVC profile

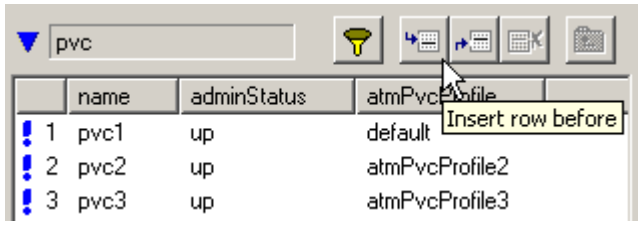
Refer to 7.1.1 - Introducing ATM on page 117 for an introduction on PVC, VPI and VCI.

In an ATM network you can set-up PVCs. A PVC allows direct connectivity between sites. In this way, a PVC is similar to a leased line. A PVC guarantees availability of a connection and does not require call setup procedures between the ATM switches.

To configure an ATM PVC, proceed as follows:

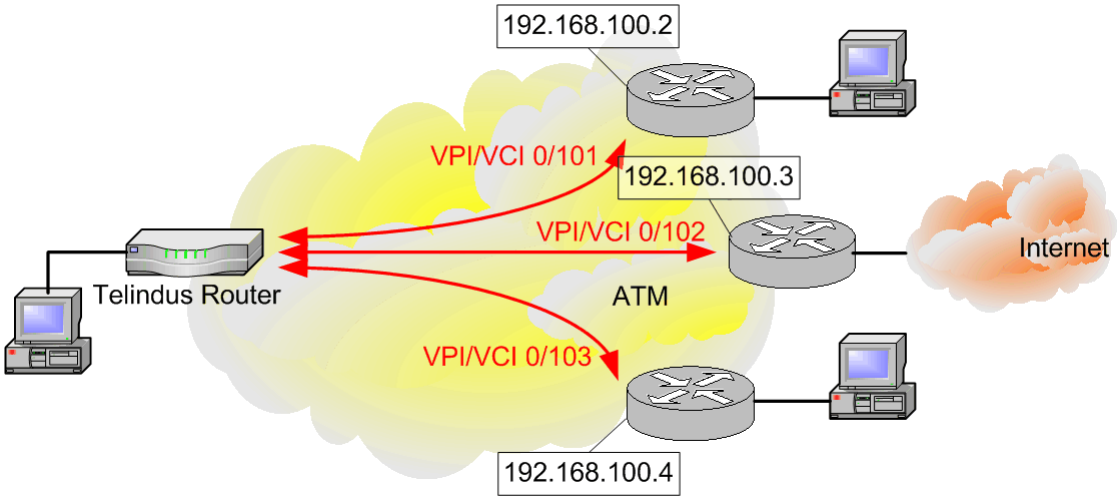
Step	Action
1	First create and configure a forwarding profile (routing or bridging). Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
2	Create an ATM PVC profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
3	Configure the attributes of the ATM PVC profile you just created. These attributes are: • vpi. Use this element to set the Virtual Path Identifier of the PVC. • vci. Use this element to set the Virtual Channel Identifier of the PVC. • qos. Use this attribute to select a Quality of Service (UBR). • oamF5Loopback. Use this element to configure the transmission of OAM F5 loop-back cells on the virtual channel. • higherLayerProtocol. Use this element to determine which higher layer protocol is used on the PVC (RFC2684 or PPPoA). • mode. Use this element to determine which forwarding profile is used on the PVC (routing, bridging or switching). Refer to 5.2.2 - How to apply the forwarding profile? on page 77. • maxFifoQLen. Use this attribute to set the maximum length (number of packets) of the First In First Out queue. Refer to 13.10.3 - ATM PVC profile configuration attributes on page 369 for more information on the configuration attributes of the ATM PVC profile.

Step	Action
4	Create a line configuration profile. Refer to 5.2.3 - How to create a line configuration profile? on page 79.
5	Configure the attributes of the line configuration profile you just created. These attributes are: • xdslProfile (where xdsl is adsl and shdsl). Use this attribute to determine which xDSL profile is used in the line configuration profile (and eventually on the xDSL line). Refer to 5.2.4 - How to apply the xDSL and ATM PVC profiles? on page 80. • pvc. Use this attribute to determine which profile is applied on each ATM PVC. So you have to add an entry to the pvc table for every ATM PVC that you want to create (on a specific xDSL line). Refer to 5.2.4 - How to apply the xDSL and ATM PVC profiles? on page 80. • vp. Use this attribute to configure the transmission of OAM F4 loop-back cells on the virtual path. Refer to 13.10.8 - Line configuration profile configuration attributes on page 395 for more information on the configuration attributes of the line configuration profile.
6	Eventually, before the previously created ATM PVCs become truly active, you have to apply the line configuration profile you just created on an xDSL line. Refer to 5.2.5 - How to apply the line configuration profile? on page 82.

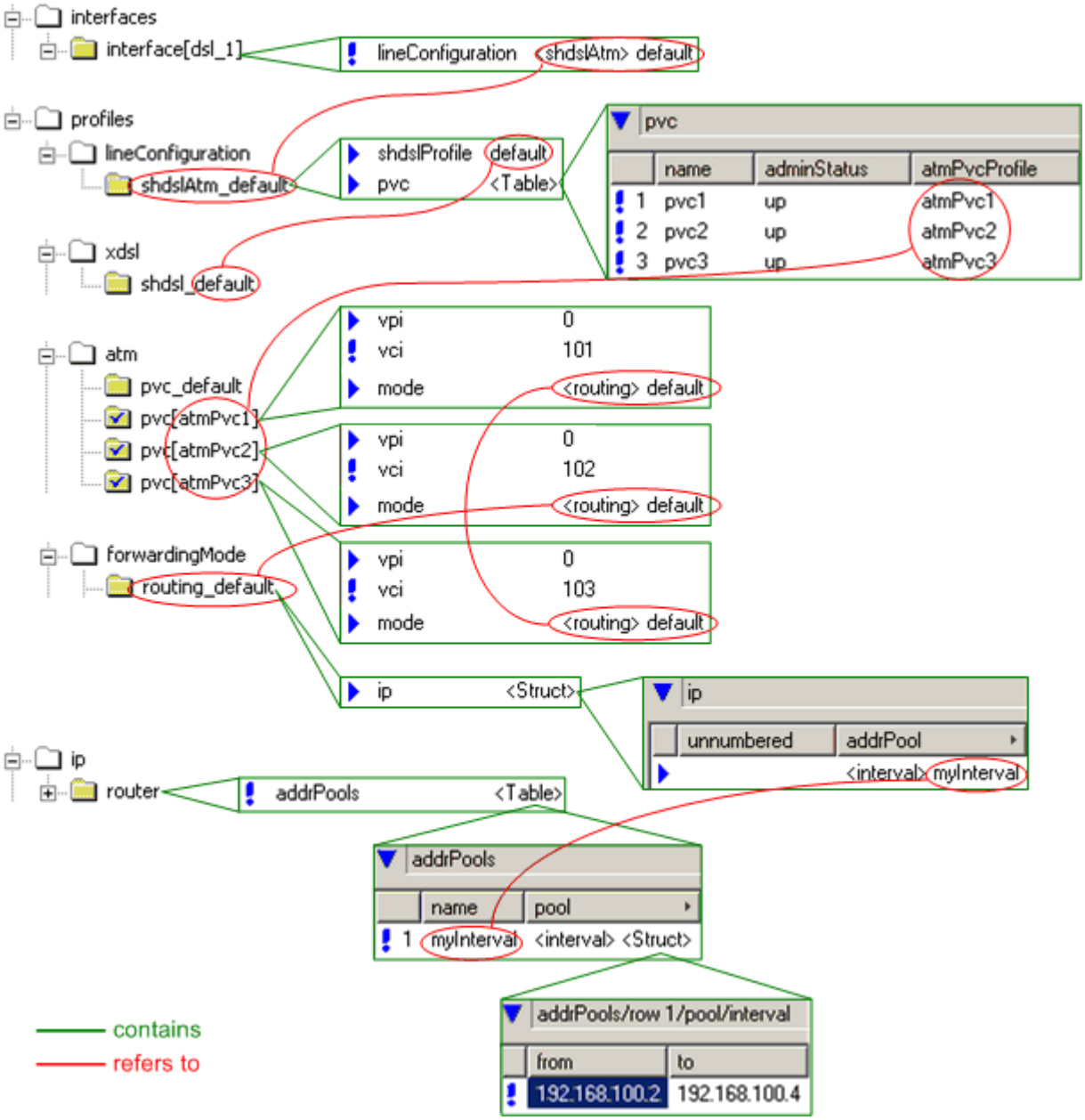


Example - configuring ATM PVCs

The following figure shows a set-up where a LAN network is connected to three different networks through three different PVCs.



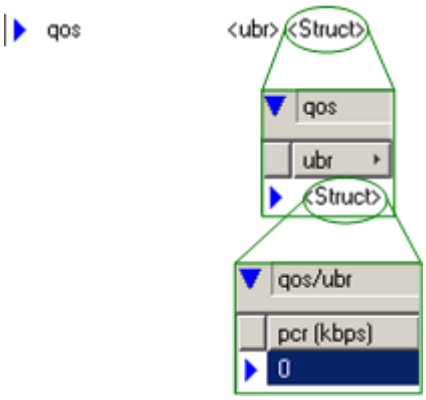
The following figure shows how to configure the ATM PVCs.



7.1.5 Configuring UBR

Refer to 7.1.1 - Introducing ATM on page 117 for an introduction on UBR and related traffic parameters.

To configure UBR, configure your ATM PVC profile as follows:

Step	Action
1	Set the first part of the qos attribute value to ubr. ⇒In the second part of the qos attribute value the string <Struct> appears.
2	In the ubr structure, configure the UBR related traffic parameters. The only parameter you have to configure in case of UBR is the Peak Cell Rate (PCR). The PCR only provides an indication of a physical bandwidth limitation within a PVC. 

Refer to telindus24xx/profiles/atm/pvc_default/qos on page 370 for a complete explanation of the qos attribute.

Over-dimensioning the PCR

In case you over-dimension the PCR, the Telindus 2400 can (proportionally) redistribute the bandwidth over the different PVCs. Refer to 7.1.7 - ATM PVC bandwidth redistribution on page 131.

When you do exceed the total bandwidth of the physical connection, then the Telindus 2400 first buffers the data. However, when the buffers of the Telindus 2400 are completely filled up, it has to discard the “excess” data.

Important remark

Per definition, the PCR is the specified amount of unguaranteed bandwidth. However, you could set a guaranteed bandwidth using the PCR. To do so …

- do not over-dimension the PCR (i.e. do not let the sum of the PCRs of the PVCs exceed the bandwidth of the physical connection).
- do not set the PCR to auto.

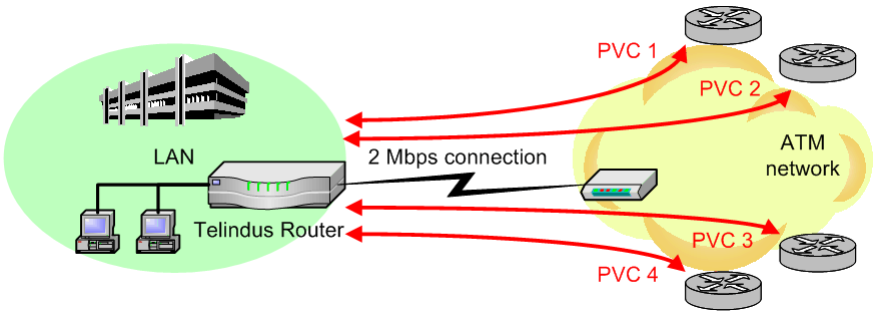
7.1.6 ATM PVC bandwidth redistribution

In ATM, the bandwidth assigned to each PVC is recalculated at regular intervals. This means that depending on the traffic on the PVCs, the Telindus 2400 can (proportionally) divide the bandwidth over the different PVCs. As a result, over-dimensioning the PCR on ATM is not as fatal as over-dimensioning the CIR on Frame Relay. The following examples will clarify this.

Examples

Suppose you have a 2 Mbps physical connection towards the ATM service provider and you define 4 PVCs.

The following tables show some possible scenarios.



PCR = auto scenarios

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	2048 kbps	512 kbps
PVC 3	auto	2048 kbps	512 kbps
PVC 4	auto	2048 kbps	512 kbps

⇒Because all PCRs are set to auto, each PVC tries to get a maximum bandwidth. Hence, the total available bandwidth (2 Mbps) is divided equally over the four PVCs.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	1024 kbps	512 kbps
PVC 3	auto	640 kbps	512 kbps
PVC 4	auto	512 kbps	512 kbps

⇒Because all PCRs are set to auto, each PVC tries to get a maximum bandwidth. Hence, the total available bandwidth (2 Mbps) is divided equally over the four PVCs. So in this scenario, PVC 4 is the only one that gets all of its data on the ATM network.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	auto	2048 kbps	2048 kbps
PVC 2	auto	0	0
PVC 3	auto	0	0
PVC 4	auto	0	0

⇒Because PVC 1 is the only one sending data and because its PCR is set to auto, it gets the total available bandwidth (2 Mbps) and is able to send its data at 2048 kbps.

PCR = fixed scenarios

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	1024 kbps	2048 kbps	1024 kbps
PVC 2	512 kbps	2048 kbps	512 kbps
PVC 3	448 kbps	2048 kbps	448 kbps
PVC 4	64 kbps	2048 kbps	64 kbps

⇒Because the sum of the PCRs equals the total available bandwidth (2 Mbps), all the PVCs get the bandwidth that is specified in their PCRs.

Scenario:

	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	2048 kbps	2048 kbps	1024 kbps
PVC 2	1024 kbps	2048 kbps	512 kbps
PVC 3	512 kbps	2048 kbps	256 kbps
PVC 4	512 kbps	2048 kbps	256 kbps

⇒In this case the PCRs of the PVCs are over-dimensioned (i.e. the sum of the PCRs exceeds the bandwidth of the physical connection towards the ATM network). What is more, the total amount of data that the PVCs try to send also exceeds the total amount of available bandwidth.
As a result, the total available bandwidth (2 Mbps) is divided proportionally over the PVCs: 2048 kbps is the total available bandwidth and 512 kbps is the lowest speed. So PVC 1 gets 4/8th (1024 kbps) of the total available bandwidth, PVC 2 gets 2/8th (512 kbps), PVC 3 and 4 each get 1/8th (256 kbps).

Scenario:

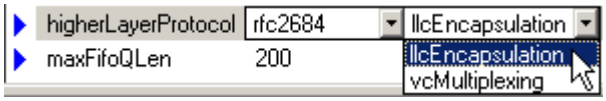
	Configured PCR	Amount of data sent	Assigned bandwidth
PVC 1	2048 kbps	2048 kbps	896 kbps
PVC 2	2048 kbps	2048 kbps	896 kbps
PVC 3	512 kbps	2048 kbps	192 kbps
PVC 4	1024 kbps	64 kbps	64 kbps

⇒In this case the PCRs of the PVCs are over-dimensioned (i.e. the sum of the PCRs exceeds the bandwidth of the physical connection towards the ATM network). What is more, the total amount of data that the PVCs try to send also exceeds the total amount of available bandwidth. However, one PVC (PVC 4) does not use the bandwidth as specified in its PCR.
As a result, the total available bandwidth (2 Mbps) is divided proportionally over the PVCs. The “spare” bandwidth that PVC 4 does not use is also proportionally divided over the three PVCs which can use this extra bandwidth (PVC 1, 2 and 3).

7.1.7 Configuring bridged/routed Ethernet/IP over ATM (RFC 2684)

Refer to 7.1.1 - Introducing ATM on page 117 for an introduction on bridged/routed Ethernet/IP over ATM.

To configure bridged/routed Ethernet/IP (multi-protocol) over ATM, configure your ATM PVC profile as follows:

Step	Action
1	Set the first part of the higherLayerProtocol attribute value to rfc2684. By selecting this value you indicate that different types of protocol data units (PDUs) may be present in the traffic on this interface.
2	Set the second part of the higherLayerProtocol attribute value to the desired encapsulation technique.  By selecting one of these two values you indicate how the different types of protocol data units (PDUs) have to be encapsulated in ATM AAL type 5. In case of … • llcEncapuslation, all the different PDU types are carried over a single PVC. In this case, the different PDU types can be distinguished from one another by the information in the Logical Link Control (LLC) header. • vcMultiplexing, each PDU type is carried over a separate PVC. So in this case, you have to set up as many PVCs as there are PDU types in your traffic. What is more, the remote application has to know which PVC carries which PDU type.

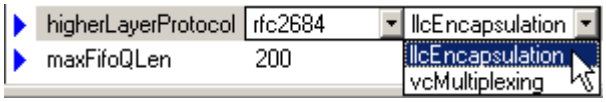
Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol on page 372 for a complete explanation of the higherLayerProtocol attribute.

7.1.8 Configuring Classical IP (IPoA)

Refer to 7.1.1 - Introducing ATM on page 117 for an introduction on IP over ATM.

Classical IP (RFC 1577) is one of the first commonly used encapsulations of IP over ATM. The encapsulation method is the same as described in RFC 2684 (formerly RFC 1483). The IP traffic is encapsulated without Ethernet header. Inverse ARP is in use for the resolution of IP addresses to PVC channels.

To configure Classical IP, configure your ATM PVC profile as follows:

Step	Action
1	Use the mode attribute to select a routing forwarding profile.
2	Set the first part of the higherLayerProtocol attribute value to rfc2684.
3	Set the second part of the higherLayerProtocol attribute value to the desired encapsulation mechanism: llcEncapuslation or vcMultiplexing. 

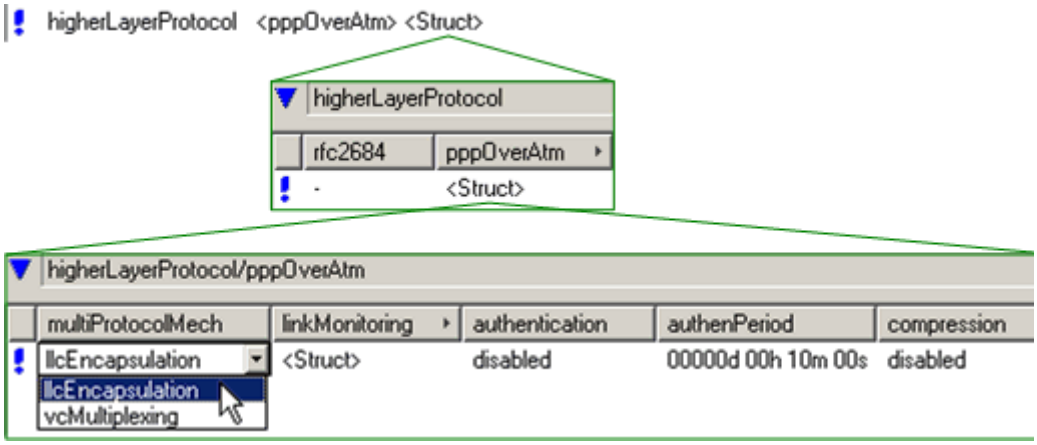
Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol on page 372 for a complete explanation of the higherLayerProtocol attribute.

Note that Inverse ARP is always in use. Therefore there is no dedicated attribute to enable or disable InARP.

7.1.9 Configuring PPP over ATM (PPPoA)

Refer to 7.1.1 - Introducing ATM on page 117 for an introduction on PPP over ATM.

To configure PPP over ATM, configure your ATM PVC profile as follows:

Step	Action
1	Set the first part of the higherLayerProtocol attribute value to pppOverAtm. ⇒In the second part of the higherLayerProtocol attribute value the string <Struct> appears.
2	In the pppOverAtm structure, set the multiProtocolMech element to the desired encapsulation mechanism: llcEncapuslation or vcMultiplexing. 
3	In the pppOverAtm structure, configure the remaining PPP related attributes (link monitoring, authentication, etc.). Refer to … • telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm> on page 373 for an overview of the elements in the pppOverAtm structure. • 7.2 - Configuring PPP encapsulation (in case of PPPoA) on page 137 for more information on configuring PPP.

7.2 Configuring PPP encapsulation (in case of PPPoA)

When using PPP over ATM (refer to What is PPPoA (RFC 2364)? on page 122), it is possible that you have to configure some PPP related configuration attributes. Therefore, this section introduces the PPP encapsulation protocol and gives a short description of the attributes you can use to configure this encapsulation protocol. To find out how to enable PPPoA, refer to 7.1.10 - Configuring PPP over ATM (PPPoA) on page 136.

The following gives an overview of this section:

- 7.2.1 - Introducing PPP on page 138
- 7.2.2 - Automatically obtaining IP addresses in PPP on page 141
- 7.2.3 - Configuring IP addresses in PPP on page 143
- 7.2.4 - Imposing IP addresses on the remote in PPP on page 144
- 7.2.5 - Configuring link monitoring on page 145
- 7.2.6 - Configuring PAP on page 146
- 7.2.7 - How does PAP work? on page 147
- 7.2.8 - Configuring CHAP on page 149
- 7.2.9 - How does CHAP work? on page 150

7.2.1 Introducing PPP

What is PPP?

The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for assigning and managing IP addresses, asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for added networking capabilities.

Also refer to What is PPPoA (RFC 2364)? on page 122.

What is LCP, IPCP, BCP and CCP?

PPP provides a method for transmitting datagrams over serial point-to-point links, which include the following components:

- A method for encapsulating datagrams over serial links.
- An extensible Link Control Protocol (LCP) which provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection.
- A family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols such as the IP Control Protocol (IPCP) and the Bridge Control Protocol (BCP).
- A Compression Control Protocol (CCP) for configuring, enabling and disabling data compression algorithms on both ends of the point-to-point link.

The PPP handshake

PPP makes a handshake in two phases:

Phase	Description
1	The Link Control Protocol (LCP) builds the link layer.
2	The Network Control Protocol (NCP, i.e. IPCP or BCP) builds the network layer.

What is PPP link monitoring?

PPP features link monitoring in order to whether the PPP link is truly up or down. If link monitoring is enabled, then echo request packets are sent over the link at regular intervals. If on consecutive requests no reply is given, then the PPP link is declared down. Data traffic is stopped until the PPP handshake succeeds again.

What is PAP?

The Password Authentication Protocol (PAP) is the most basic form of authentication (complies with RF 1334). It basically works the same way as a normal login procedure. The peer (the authenticating system) authenticates itself by sending a user name and password to the authenticator. The authenticator compares this user name and password to its secrets database. If the password matches, the peer is authenticated and the session can be set up. PAP authentication can be performed in one direction or in both directions.

The disadvantage of PAP is that it is vulnerable to eavesdroppers who may try to obtain the password by listening in on the serial line, and to repeated trial and error attacks.

What is CHAP?

The Challenge Handshake Authentication Protocol (CHAP) is more secure than PAP.

With CHAP, the server (the authenticator) sends a randomly generated “challenge” string to the client (the authenticating system). The client hashes the challenge string, its user name and password using the MD5 algorithm. This result is returned to the server. The server now performs the same computation and compares this user name and password to its secrets database. If the passwords match, the client is authenticated and the session can be set up. CHAP authentication can be performed in one direction or in both directions.

Another feature of CHAP is that it does not only requires the client to authenticate itself at start-up time, but to do so at regular intervals. This to make sure the client has not been replaced by an intruder (for instance by just switching lines).

What is MS-CHAP?

The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication. In this case, authentication occurs between a PC using Microsoft Windows and a router or access server acting as a network access server (NAS).

The differences between the standard CHAP and MS-CHAP are:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set a "reason for failure" codes returned in the Failure packet message field.

What is MS-CHAP v2?

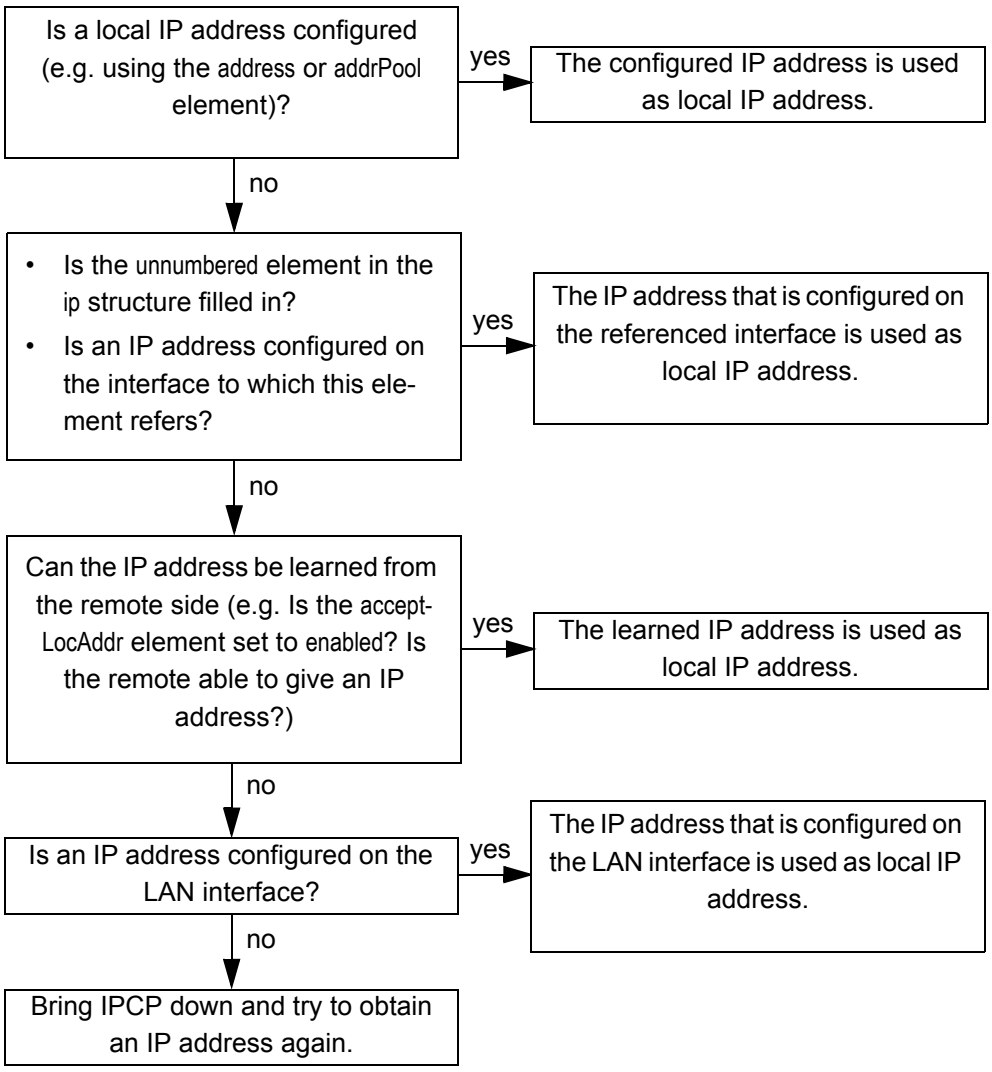
MS-CHAP version 2 provides stronger security for remote access connections and also solves some issues of MS-CHAP version 1:

MS-CHAP version 1 issue	MS-CHAP version 2 solution
LAN Manager encoding of the response used for backward compatibility with older Microsoft remote access clients is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded responses.
LAN Manager encoding of password changes is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded password changes.
Only one-way authentication is possible. The remote access client cannot verify that it is dialling in to its organisation's remote access server or a masquerading remote access server.	MS-CHAP v2 provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialling in to has access to the user's password.
With 40-bit encryption, the cryptographic key is based on the user's password. Each time the user connects with the same password, the same cryptographic key is generated.	With MS-CHAP v2, the cryptographic key is always based on the user's password and an arbitrary challenge string. Each time the user connects with the same password, a different cryptographic key is used.
A single cryptographic key is used for data sent in both directions on the connection.	With MS-CHAP v2, separate cryptographic keys are generated for transmitted and received data.

7.2.2 Automatically obtaining IP addresses in PPP

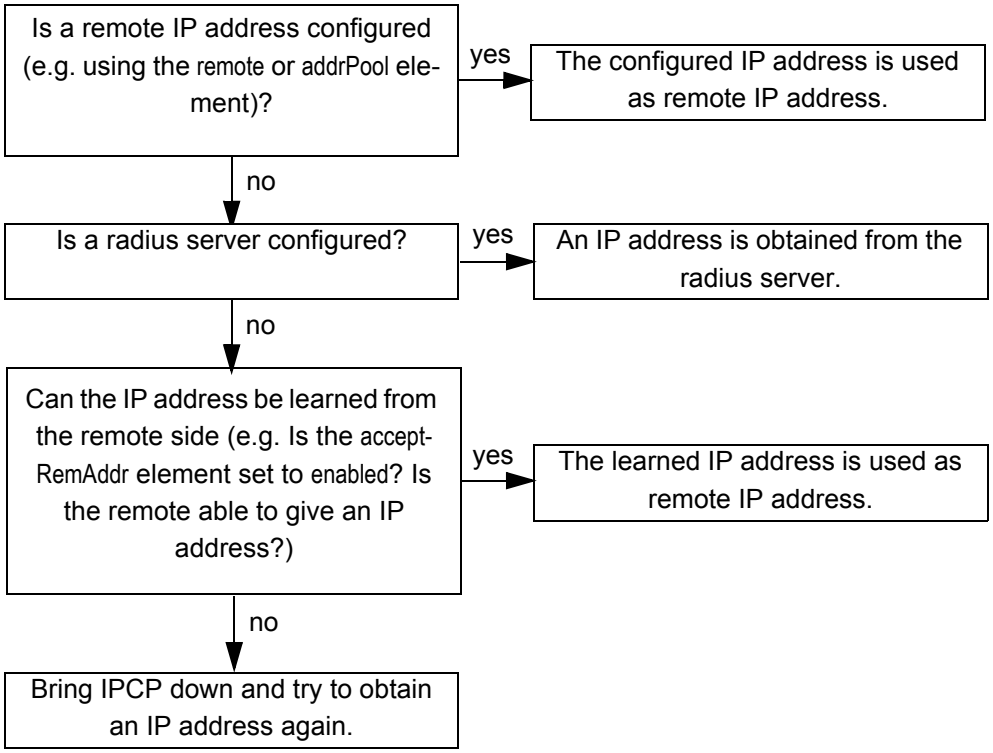
Obtaining a local IP address

In case of PPP, the Telindus 2400 can learn the local IP address of a PPP link.


Is a local IP address configured (e.g. using the address or addrPool element)?
yes
The configured IP address is used as local IP address.
no
• Is the unnumbered element in the ip structure filled in?
• Is an IP address configured on the interface to which this element refers?
yes
The IP address that is configured on the referenced interface is used as local IP address.
no
Can the IP address be learned from the remote side (e.g. Is the acceptLocAddr element set to enabled? Is the remote able to give an IP address?)
yes
The learned IP address is used as local IP address.
no
Is an IP address configured on the LAN interface?
yes
The IP address that is configured on the LAN interface is used as local IP address.
no
Bring IPCP down and try to obtain an IP address again.

Obtaining a remote IP address

In case of PPP, the Telindus 2400 can learn the remote IP address of a PPP link.


Is a remote IP address configured (e.g. using the remote or addrPool element)?
yes
The configured IP address is used as remote IP address.
no
Is a radius server configured?
yes
An IP address is obtained from the radius server.
no
Can the IP address be learned from the remote side (e.g. Is the acceptRemAddr element set to enabled? Is the remote able to give an IP address?)
yes
The learned IP address is used as remote IP address.
no
Bring IPCP down and try to obtain an IP address again.

7.2.3 Configuring IP addresses in PPP

To configure IP addresses on a PPPoA link, proceed as follows:

Step	Action
1	First create a routing forwarding profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
2	In the routing forwarding profile you just created, configure the ip structure. It is in this structure that you can configure the IP addresses (and other IP related attributes). The most important elements of the ip structure are: • unnumbered. Use this element to “borrow” an IP address from another interface. • addrPool. Use this element to pick an IP address out of an IP address pool. • acceptLocAddr. This applies on PPPoA links only. Use this element to determine whether to accept or reject the local IP address being imposed by the remote side. • acceptRemAddr. This applies on PPPoA links only. Use this element to determine whether to accept or reject the remote IP address being imposed by the remote side. Refer to 6.2.3 - Explaining the ip structure on page 90 for a detailed explanation of the elements in the ip structure. **Important remark** In the ip structure for the PPP(oA) protocol on the … • xDSL lines, the gatewayPreference element *is not* present. This because on this side the Telindus 2400 is the “central” device (links towards the remote access routers). A central device typically does not have a default gateway to a remote. • 6E1 and E3/T3 interface on the other hand, the gatewayPreference element *is* present. This because on this side the Telindus 2400 is the “remote” device (uplink towards the backbone network). A remote device typically has a default gateway to a central device.
3	Create an ATM PVC profile. Refer to 5.2.1 - How to create an xDSL, ATM PVC and forwarding profile? on page 75.
4	Apply the routing forwarding profile on the ATM PVC profile. Refer to 5.2.2 - How to apply the forwarding profile? on page 77. ⇒By doing so, you configured the IP addresses of one ATM PVC. However, before this ATM PVC becomes active, you still have to add it to the PVC table and apply it on an xDSL line. Refer to 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126.

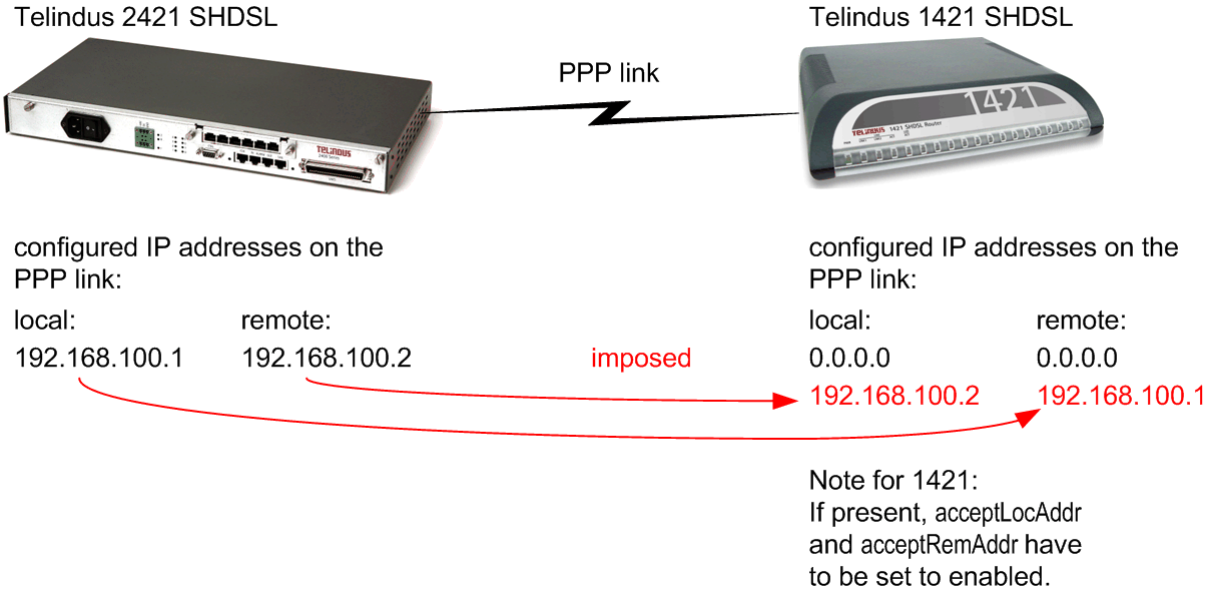
7.2.4 Imposing IP addresses on the remote in PPP

As can be seen in 7.2.2 - Automatically obtaining IP addresses in PPP on page 141, in case of PPP the Telindus 2400 can learn IP addresses from the remote side. What is more, in case of PPP the Telindus 2400 itself can impose IP addresses on the remote.

To impose IP addresses on the remote, proceed as follows:

Step	Action
1	On the Telindus 2400, configure a local and remote IP address on the PPP link. Refer to 7.2.3 - Configuring IP addresses in PPP on page 143.
2	On the remote device (e.g. a Telindus 1421 SHDSL), configure nor a local nor a remote address on the PPP link. ⇒Once the PPP handshake reaches the IPCP stage, the Telindus 1421 SHDSL will declare to the Telindus 2400 that it has no IP addresses on its PPP link. The Telindus 2400 on its turn will impose the local and remote IP address of the PPP link on the Telindus 1421 SHDSL. Note that should the IP configuration attributes acceptLocAddr and acceptRemAddr be present on the Telindus 1421 SHDSL, then they have to be set to enabled. Else the Telindus 1421 SHDSL will not accept the IP addresses imposed by the Telindus 2400.

Example - imposing IP addresses on the remote in PPP



7.2.5 Configuring link monitoring

Refer to 7.2.1 - Introducing PPP on page 138 for an introduction on link monitoring.

To configure link monitoring, configure the PPP attributes as follows:

Step	Action
1	Configure your ATM PVC profile for PPP over ATM. Refer to 7.1.10 - Configuring PPP over ATM (PPPoA) on page 136.
2	In the pppOverAtm structure, enter the linkMonitoring structure.
3	The linkMonitoring structure contains the following elements: • operation. Use this element to enable or disable link monitoring. • interval. Use this element to set the time interval between two consecutive echo requests. • replyTimeOut. Use this element to set the time the Telindus 2400 waits for a reply on the echo request. • failsPermitted. Use this element to set the number of echo requests that may fail before the Telindus 2400 declares the PPP link down. Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm> on page 373 for more information on the elements of the linkMonitoring configuration structure.

7.2.6 Configuring PAP

Refer to 7.2.1 - Introducing PPP on page 138 for an introduction on PAP.

Important remark

In the PPP(oA) protocol on the …

- xDSL lines, the Telindus 2400 is always the authenticator, never the peer.
- TIMs (Telindus Interface Module) on the other hand, the Telindus 2400 can be both authenticator and peer.

To configure PAP, configure the PPP attributes as follows:

Step	Action
1	Configure your ATM PVC profile for PPP over ATM. Refer to 7.1.10 - Configuring PPP over ATM (PPPoA) on page 136.
2	In the pppOverAtm structure, configure the following elements: • authentication. Use this element to set the PPP authentication to PAP. • authenPeriod. Use this element to determine the interval at which the PPP link is authenticated once it has been set up. Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm> on page 373 for more information on the elements of the pppOverAtm configuration structure.
3	In the telindus24xx/ip/router object, configure the pppSecretTable. Enter the name and secret of the peer in this table.

How exactly all these configuration attributes are used in the authentication process is explained in the 7.2.7 - How does PAP work? on page 147.

7.2.7 How does PAP work?

Refer to 7.2.1 - Introducing PPP on page 138 for an introduction on PAP.

PAP authentication in one direction

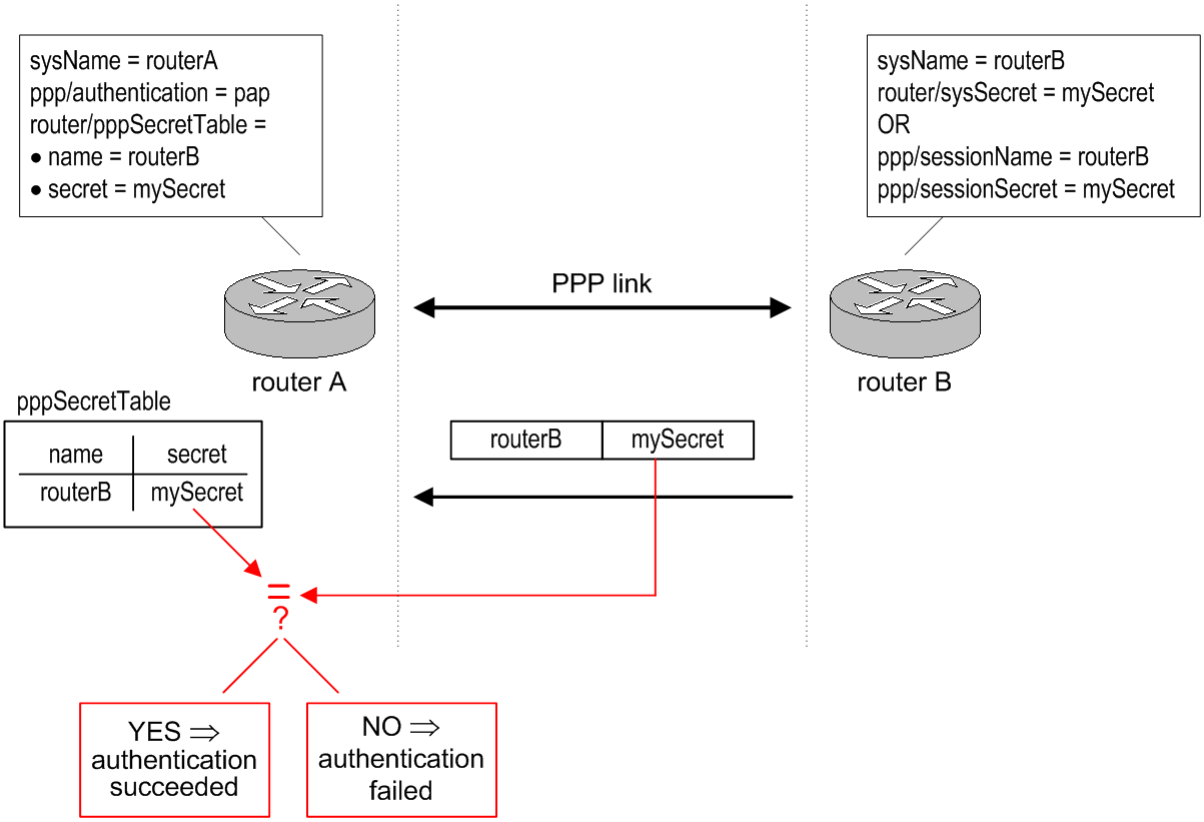
The router authenticates after building its LCP layer and prior to building the IPCP layer. If the authentication succeeds, then the PPP link is built further until data can be sent. Else PPP starts its handshake again.

Consider the following example: router A (the Telindus 2400) is the authenticator and router B is the peer. Router A is configured for PAP authentication and router B is not. The authentication process goes as follows:

Phase	Description
1	Router B wants to establish a PPP link with router A (the Telindus 2400).
2	Router A asks router B to authenticate himself.
3	Router B sends its name[1] and its secret[2] to router A.
4	Router A looks up the name of router B in its pppSecretTable to find a corresponding secret. If the secret found in the pppSecretTable matches the secret received from router B, then the authentication succeeded and a PPP link is established. Else the authentication failed and no PPP link is established.

1. Depending on how router B is configured, this can be its sysName or sessionName.
2. Depending on how router B is configured, this can be its sysSecret or sessionSecret.

The following figure shows the PAP authentication process:



PAP authentication in both directions

If PAP authentication is enabled on both routers, then they both request and respond to the authentication. If the remote router is a router from another vendor, then read the documentation in order to find out how to configure the PAP name and secret values.

7.2.8 Configuring CHAP

Refer to 7.2.1 - Introducing PPP on page 138 for an introduction on CHAP.

Important remark

In the PPP(oA) protocol on the …

- xDSL lines, the Telindus 2400 is always the authenticator, never the peer.
- TIMs (Telindus Interface Module) on the other hand, the Telindus 2400 can be both authenticator and peer.

To configure CHAP, configure the PPP attributes as follows:

Step	Action
1	Configure your ATM PVC profile for PPP over ATM. Refer to 7.1.10 - Configuring PPP over ATM (PPPoA) on page 136.
2	In the pppOverAtm structure, configure the following elements: • authentication. Use this element to set the PPP authentication to CHAP (or MS-CHAP or MS-CHAP v2). • authenPeriod. Use this element to determine the interval at which the PPP link is authenticated once it has been set up. Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm> on page 373 for more information on the elements of the pppOverAtm configuration structure.
3	In the telindus24xx/ip/router object, configure the pppSecretTable. Enter the name and secret of the peer in this table.

How exactly all these configuration attributes are used in the authentication process is explained in the 7.2.9 - How does CHAP work? on page 150.

7.2.9 How does CHAP work?

Refer to 7.2.1 - Introducing PPP on page 138 for an introduction on CHAP.

CHAP authentication in one direction

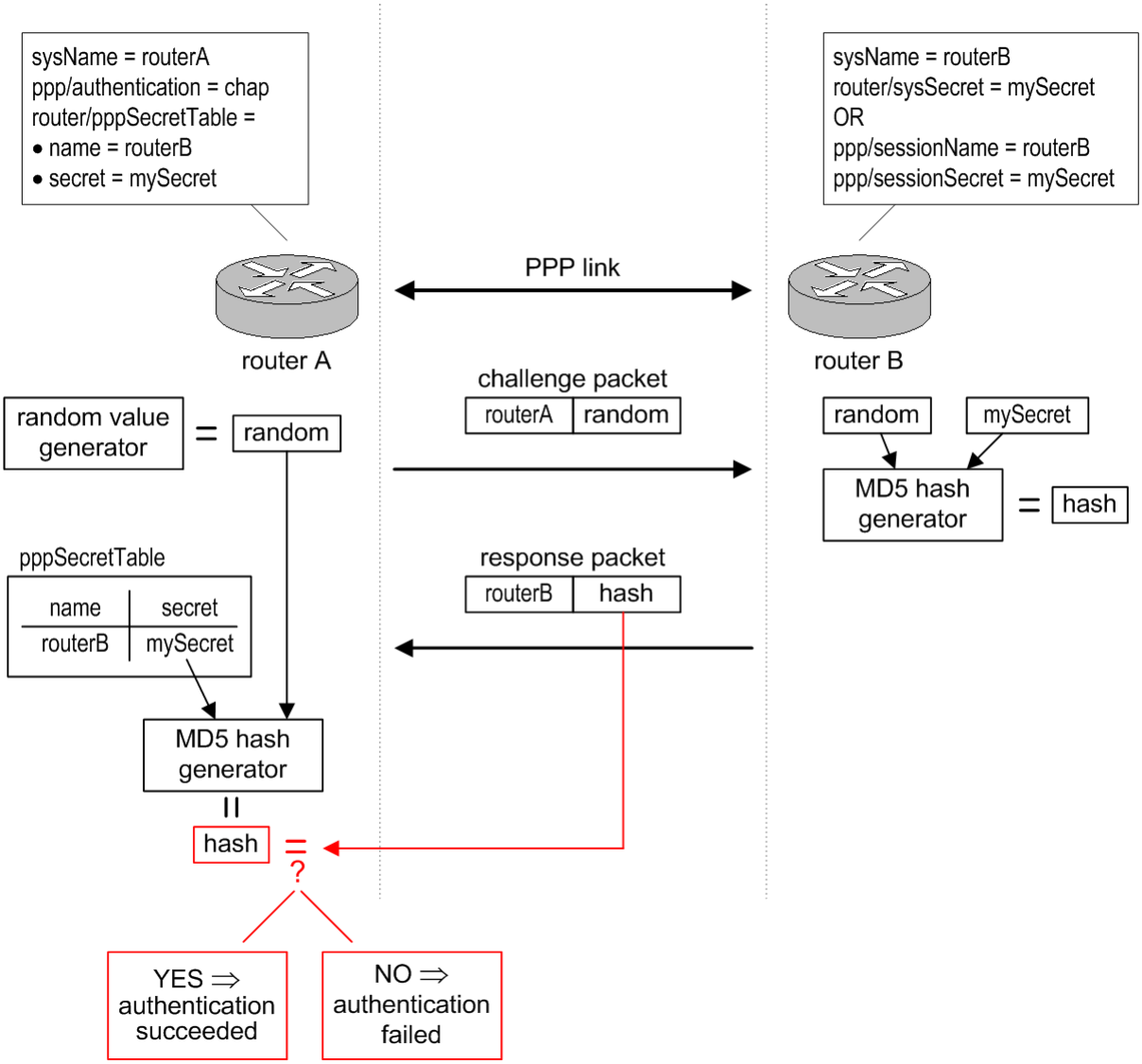
The router authenticates after building its LCP layer and prior to building the IPCP layer. If the authentication succeeds, then the PPP link is built further until data can be sent. Else PPP starts its handshake again.

Consider the following example: router A (the Telindus 2400) is the authenticator and router B is the peer. Router A is configured for CHAP authentication and router B is not. The authentication process goes as follows:

Phase	Description
1	Router B wants to establish a PPP link with router A (the Telindus 2400).
2	Router A asks router B to authenticate himself. So router A sends a challenge packet containing a random value to router B. The challenge packet also contains the sysName of router A. If the peer (router B) is also a Telindus Router, then it does nothing with it. Other vendors, however, may use this sysName to determine which secret to use in the authentication process. Check the vendor's documentation.
3	Router B feeds the random value and its secret[1] into the MD5 hash generator, resulting in a hash value.
4	Router B sends a response packet containing the hash value and its name[2].
5	Router A looks up the name of router B in its pppSecretTable to find a corresponding secret. This secret found in the pppSecretTable and the random value router A sent in step 2 is fed into the MD5 hash generator, resulting in a hash value. If this hash value equals the hash value received from router B, then the authentication succeeded and a PPP link is established. Else the authentication failed and no PPP link is established.

1. Depending on how router B is configured, this can be its sysSecret or sessionSecret.
2. Depending on how router B is configured, this can be its sysName or sessionName.

The following figure shows the authentication process:



CHAP authentication in both directions

If CHAP authentication is enabled on both routers, then they both request and respond to the authentication. If the remote router is a router from another vendor, then read the documentation in order to find out how to configure the CHAP name and secret values.

8 Configuring the encapsulation on the TIMs

This chapter introduces the encapsulation protocols that you can use on the TIMs (Telindus Interface Modules) and lists the attributes you can use to configure the encapsulation protocols.

The following gives an overview of this chapter:

- 8.1 - Configuring IMA on the 6E1 interface on page 154
- 8.2 - Configuring ATM on the E3/T3 interface on page 159

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

8.1 Configuring IMA on the 6E1 interface

Inserting a 6E1 interface in the empty interface slot of the Telindus 2400 allows you to connect the Telindus 2400 to a backbone network through this interface. The encapsulation protocol that can be used on the 6E1 interface is Inverse Multiplexing for ATM (IMA). This chapter introduces IMA and lists the attributes you can use to configure IMA.

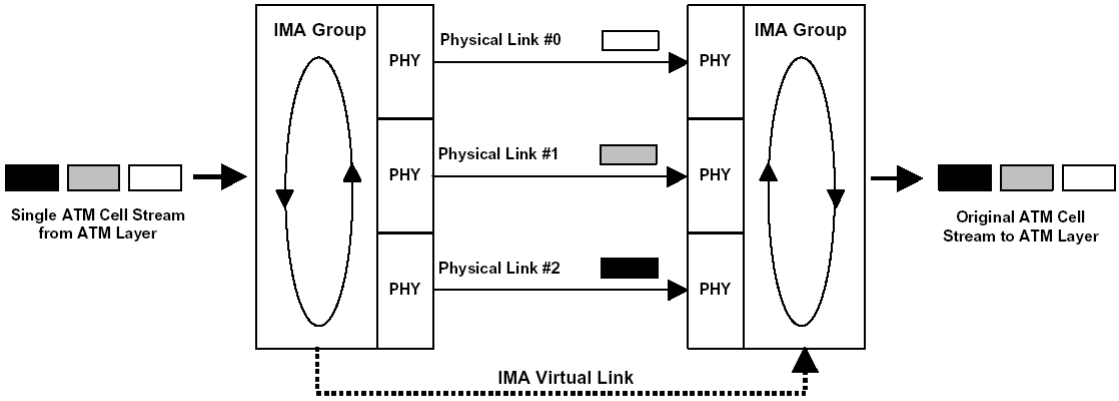
The following gives an overview of this chapter:

- 8.1.1 - Introducing IMA on page 155
- 8.1.2 - How to configure IMA? on page 156

8.1.1 Introducing IMA

What is IMA?

Inverse Multiplexing for ATM (IMA) provides inverse multiplexing of an ATM cell stream over multiple physical links and retrieves the original stream at the far-end from these physical links. The multiplexing of the ATM cell stream is performed on a cell by cell basis across the multiple physical links.



Tx direction: cells distributed across links in round robin sequence
Rx direction: cells recombined into single ATM stream

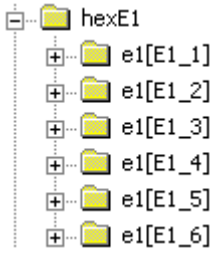
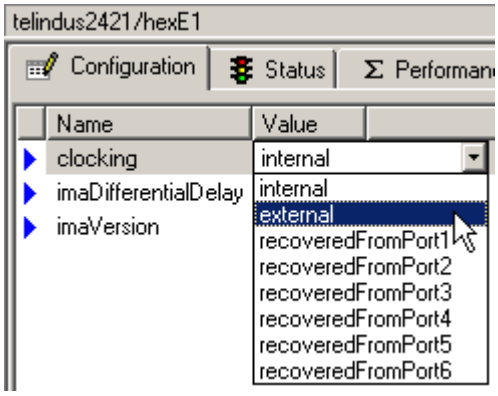
What is an IMA group?

The ATM Inverse Multiplexing technique involves inverse multiplexing and de-multiplexing of ATM cells in a cyclical fashion among links grouped to form a higher bandwidth logical link whose rate is approximately the sum of the link rates. This is referred to as an IMA group.

8.1.2 How to configure IMA?

Refer to 8.1.1 - Introducing IMA on page 155 for an introduction.

To configure IMA, proceed as follows:

Step	Action
1	If you haven't already done so, insert a 6E1 interface in the empty interface slot of the Telindus 2400. ⇒The hexE1 object appears in the containment tree. Refer to 2.6.2 - Connecting the different parts of the Telindus 2400 on page 27 for more information. 
2	Configure the general attributes of the 6E1 interface (select the hexE1 object). The most important attribute is: • ifClocking. Use this attribute to select a clocking mode. Refer to 13.6.1 - General 6E1 interface configuration attributes on page 324 for more information on the general configuration attributes of the 6E1 interface. 
3	Create an IMA group. In the Telindus 2400 containment tree, go to the bundle object and add an imaGroup[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56). E.g. imaGroup[myImaGroup]

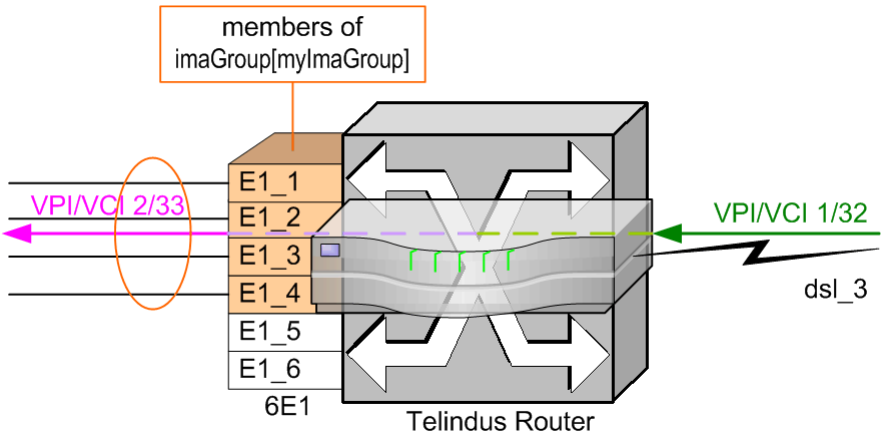
Step	Action
4	Configure the attributes of the imaGroup[ ] object you just added. The most important attributes are: • members. Use this attribute to determine which E1 interfaces are member of the IMA group. So you have to add an entry to the members table for every E1 interface that you want to include in the IMA group. Then type the index name of the E1 interface as value of the interface element. • minActiveLinks. Use this attribute to determine what the minimum amount of E1 interfaces that have to be up before the IMA group may become active. • pvc. Use this attribute to create ATM PVCs in the IMA group. So you have to add an entry to the pvc table for every ATM PVC that you want to create. Refer to 13.8 - IMA group configuration attributes on page 349 for more information on the configuration attributes of the IMA group. Note that in case you configure ATM PVCs for IMA, you do this in the pvc table which can be found in the bundle/imaGroup[ ] (refer to telindus24xx/bundle/imaGroup[ ]/pvc on page 350). In this table you find all the necessary parameters to configure the ATM PVCs. This approach differs from how you have to configure ATM PVCs on the xDSL interfaces. In that case you have to configure several profiles which are then applied on an xDSL interface.
5	Usually you will want to switch ATM PVCs from a certain xDSL interface to an IMA group (i.e. towards the backbone network). In that case you have to configure the ATM switching table. Refer to 11.3 - Configuring ATM switching on page 256 for more information on ATM switching. **Example** Suppose you want to switch ATM PVC with VPI/VCI 0/32 from xDSL interface 1 (object in containment tree: interface[dsl_1]) to an IMA group with index name mylmaGroup (object in containment tree: imaGroup[mylmaGroup]), then fill in the atm/switching table as follows: switching sourceInterface / sourceVpi / sourceVci 1 dsl_1 0 32 destinationInterface / destinationVpi / destinationVci / bidirectional mylmaGroup 0 32 yes Don't forget to set both ATM PVCs in switching mode (mode = switching).

Example - configuring IMA

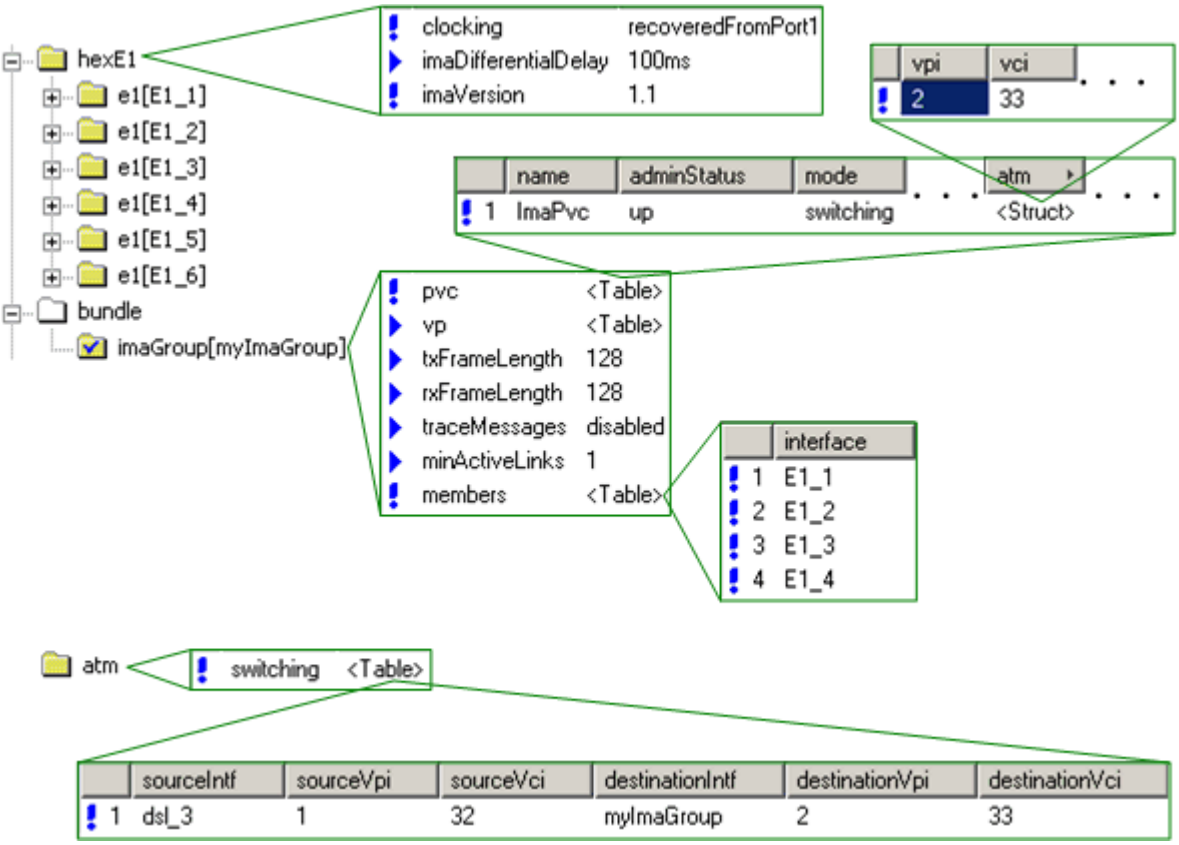
Suppose you want to …

- create an IMA group with as members E1 interface 1 up to 4 of a 6E1 interface.
- switch an ATM PVC from xDSL line 3 to the IMA group.
- recover the clock from E1 interface 1.
- use IMA version 1.1.

The following figure shows the set-up:



The following figure shows how to configure IMA:



8.2 Configuring ATM on the E3/T3 interface

Inserting an E3/T3 interface in the empty interface slot of the Telindus 2400 allows you to connect the Telindus 2400 to a backbone network through this interface. The encapsulation protocol that can be used on the E3/T3 interface is ATM. This chapter introduces ATM on the E3/T3 interface and lists the attributes you can use to configure ATM on the E3/T3 interface.

The following gives an overview of this chapter:

- 8.2.1 - Introducing ATM on the E3/T3 interface on page 160
- 8.2.2 - How to configure ATM on the E3/T3 interface? on page 161

8.2.1 Introducing ATM on the E3/T3 interface

The way you configure ATM on the xDSL interfaces is not the same as the way you configure ATM on the E3/T3 interface:

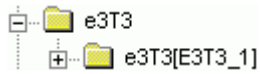
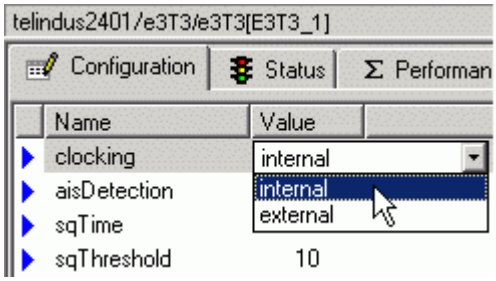
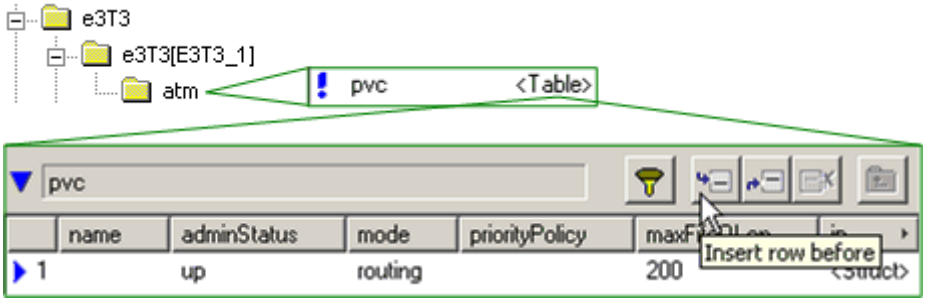
Configuring ATM on the xDSL interfaces	Configuring ATM on the E3/T3 interface
When you want to configure ATM on the xDSL interfaces you have to do this using profiles. Refer to 7.1 - Configuring ATM encapsulation on page 116.	When you want to configure ATM on the E3/T3 interface you have to do this in a PVC table. Refer to 8.2.2 - How to configure ATM on the E3/T3 interface? on page 161.

So functionally the ATM on the xDSL interfaces and on the E3/T3 interface is the same, only the way you have to configure is different.

8.2.2 How to configure ATM on the E3/T3 interface?

Refer to 8.2.1 - Introducing ATM on the E3/T3 interface on page 160 for an introduction.

To configure ATM on the E3/T3 interface, proceed as follows:

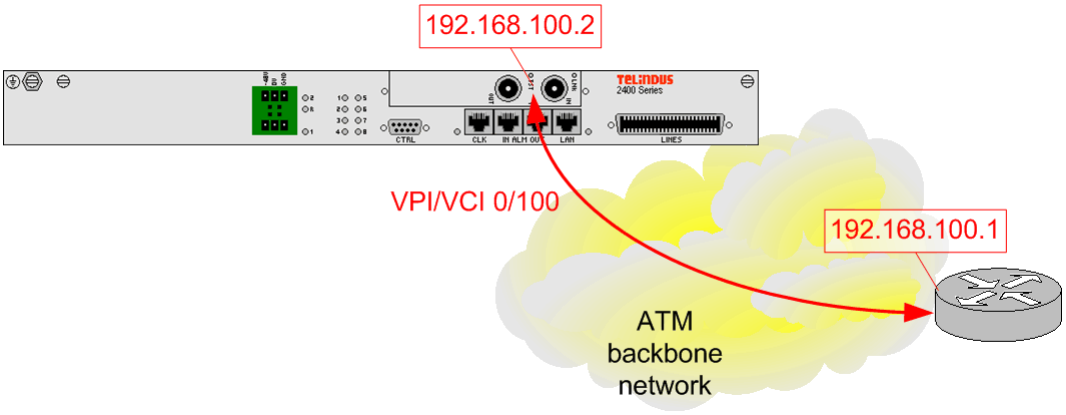
Step	Action
1	If you haven't already done so, insert an E3/T3 interface in the empty interface slot of the Telindus 2400.  ⇒The e3T3 object appears in the containment tree. Refer to 2.6.2 - Connecting the different parts of the Telindus 2400 on page 27 for more information.
2	Configure the specific attributes of the E3/T3 interface (select the e3T3/e3T3[E3T3_x] object(s)). The most important attribute is: • ifClocking. Use this attribute to select a clocking mode.  Refer to 13.7.1 - Specific E3/T3 interface configuration attributes on page 334 for more information on the specific configuration attributes of the E3/T3 interface.
3	Now go to atm object located under the e3T3[E3T3_x] object, select the pvc attribute and add one or more entries to this table.  Use this attribute to set up ATM PVCs on the E3/T3 interface. Add a row to the pvc table for each ATM PVC you want to create.
4	Configure the elements of the pvc table. The most important are: • name. Use this element to assign an administrative name to the PVC. • adminStatus. Use this element to activate or deactivate the PVC. • mode. Use this element to determine whether, for the corresponding PVC, the packets are treated by the routing process, the bridging process or the ATM switching process. • ip. Use this element to configure the IP related parameters of the PVC. • bridging. Use this element to configure the bridging related parameters of the PVC in case the PVC is in bridging mode (i.e. in case the mode element is set to bridging) • atm. Use this element to configure the ATM related parameters of the PVC. • ppp. Use this element to configure the PPP related parameters of the PVC in case you want to run PPP over ATM. Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc on page 338 for a detailed description of the pvc table.

Example - configuring ATM on the E3/T3 interface

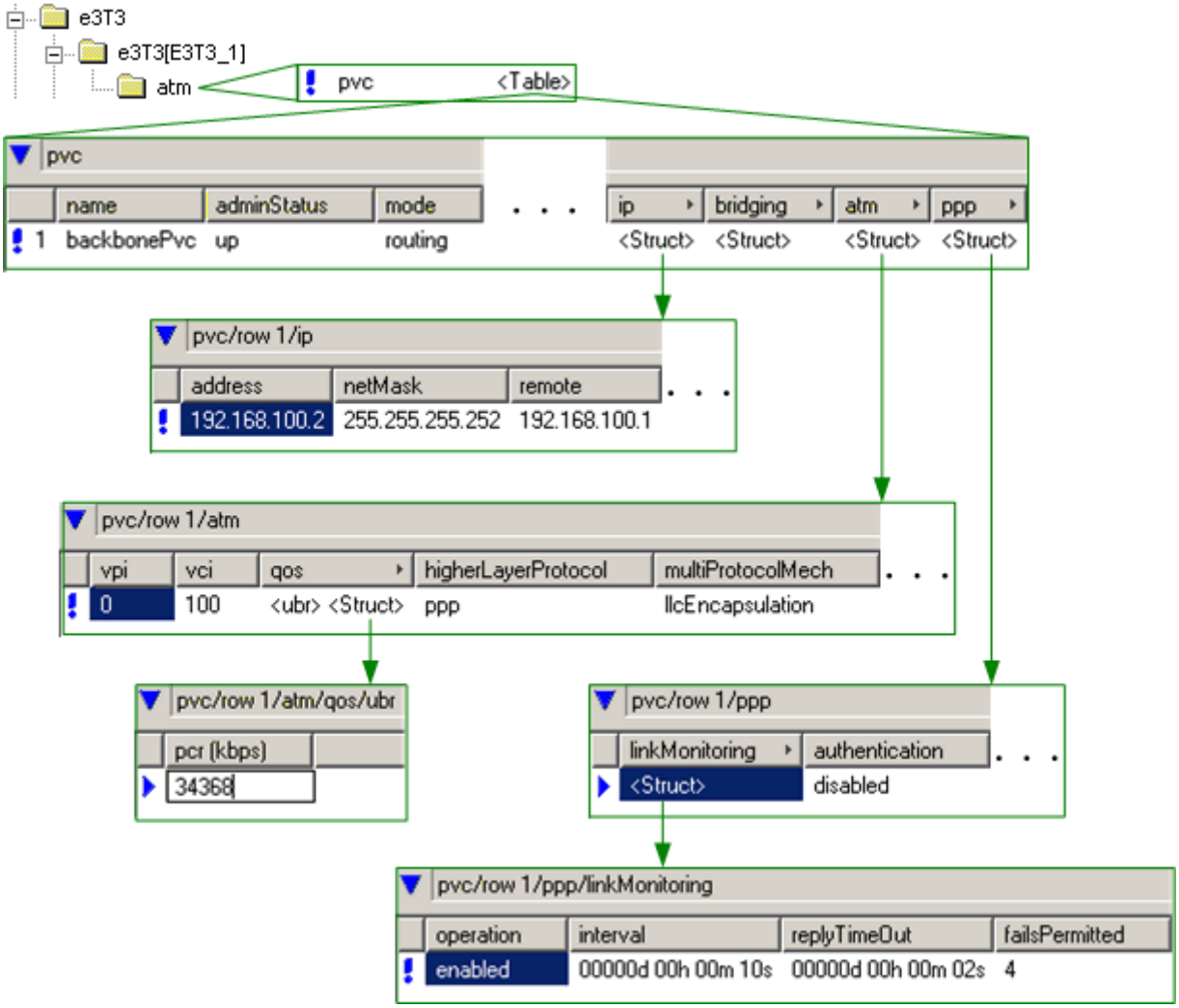
Suppose …

- you have a Telindus 2400 with an E3/T3 interface.
- the E3/T3 interface is connected to a backbone network.
- you want to configure an ATM PVC on the E3/T3 interface with the following properties:
  - name: backbonePvc
  - mode: routing
  - local IP address: 192.168.100.2
  - remote IP address: 192.168.100.1
  - VPI / VCI: 0 / 100
  - ATM service category: UBR with a PCR of 34368 kbps
  - Higher layer protocol: PPP with LLC encapsulation
  - PPPoA properties: link monitoring enabled

This is shown in the following setup:



The following figure shows how to configure the ATM PVC.



9 Configuring routing

This chapter introduces routing on the Telindus 2400 and lists the attributes you can use to configure routing.

The following gives an overview of this chapter:

- 9.1 - Introducing routing on page 166
- 9.2 - Enabling routing on an interface on page 167
- 9.3 - Configuring static routing on page 168
- 9.4 - Configuring policy based routing on page 176
- 9.5 - Configuring the Routing Information Protocol on page 182
- 9.6 - Configuring address translation on page 191
- 9.7 - Configuring traffic and priority policy on the router on page 207

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

9.1 Introducing routing

What is routing?

Routing is the act of moving information across an internetwork from a source to a destination.

Routing versus bridging

Routing is often contrasted with bridging. At first sight, bridging might seem to do the same as routing. The primary difference between the two is that bridging occurs at layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). In other words, bridging occurs at a lower level and is therefore more of a hardware function whereas routing occurs at a higher level where the software component is more important. And because routing occurs at a higher level, it can perform more complex analysis to determine the optimal path for the packet.

Basic routing activities

Routing involves two basic activities:

- determining optimal routing paths,
- transporting information groups (typically called packets).

Determining the optimal routing path

In order to determine a routing path, routers initialise and maintain routing tables. These routing tables contain a variety of information. For example:

- Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.
- Desirability of a path. Routers use metrics to evaluate what path will be the best for a packet to travel.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analysing routing updates from all other routers, a router can build a detailed picture of network topology.

Transporting packets

In most cases, a host determines that it must send a packet to another host. Having acquired a router's address by some means, the source host sends a packet addressed specifically to a router's physical (i.e. Media Access Control or MAC) address, this time with the protocol (i.e. network) address of the destination host.

As it examines the packet's destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, however, it changes the destination physical address to that of the next hop and transmits the packet.

The next hop may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the internetwork, its physical address changes, but its protocol address remains constant.

9.2 Enabling routing on an interface

Refer to 9.1 - Introducing routing on page 166 for an introduction.

Per IP interface you can determine whether you perform routing, bridging or both. The following table shows, for each IP interface, how to enable routing on this interface:

Interface	How to enable routing?
LAN interface	Set the mode attribute to routing or routingAndBridging. The mode attribute can be found in the lanInterface object: telindus24xx/lanInterface/mode. **Important remark** If you set the configuration attribute telindus24xx/lanInterface/mode to bridging (default setting!), then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. So in this particular case, if you want to manage the Telindus 2400 via IP, then you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.
4 port Ethernet interface	Set the mode attribute to routing or routingAndBridging. The mode attribute can be found in the 4pEth object: telindus24xx/4pEth/mode.
VLAN on the LAN interface	Set the mode element to routing. The mode element can be found in the vlan table which is located in the lanInterface object: telindus24xx/lanInterface/vlan/mode.
VLAN on the 4 port Ethernet interface	Set the mode element to routing. The mode element can be found in the vlan table which is located in the 4pEth object: telindus24xx/4pEth/vlan/mode.
ATM PVC on the xDSL lines	Set the mode attribute to routing, then determine which routing forwarding profile has to be applied on the ATM PVC profile. The mode attribute can be found in the profiles/atm/pvc_default or profiles/atm/pvc[ ] object: telindus24xx/profiles/atm/pvc_default/mode. Refer to 5.2.2 - How to apply the forwarding profile? on page 77.
ATM PVC on the 6E1 interface	Set the mode element to routing. The mode element can be found in the pvc table which is located in the imaGroup object: telindus24xx/bundle/imaGroup[ ]/pvc/mode.
ATM PVC on the E3/T3 interface	Set the mode element to routing. The mode element can be found in the pvc table which is located in the e3T3[E3T3_x]/atm object: telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/mode.
L2TP tunnel	Set the mode element to routing or routingAndBridging. The mode element can be found in the l2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/l2tpTunnels/mode.
IPSEC L2TP tunnel	Set the mode element to routing or routingAndBridging. The mode element can be found in the ipsecL2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/mode.

9.3 Configuring static routing

This section introduces static routing and gives a short description of the attributes you can use to configure static routing.

The following gives an overview of this section:

- 9.3.1 - Introducing static routing on page 169
- 9.3.2 - Configuring a default route on page 170
- 9.3.3 - Configuring the routing table on page 171
- 9.3.4 - Configuring the routing table - rules of thumb on page 174
- 9.3.5 - The rerouting principle on page 175

9.3.1 Introducing static routing

Static versus dynamic routing

The following table states the differences between static and dynamic routing:

Routing algorithm	Description
static	Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Static routing algorithms work well in environments where network traffic is relatively predictable and where network design is relatively simple.
dynamic	Because static routing systems cannot react to network changes, they generally are considered unsuitable for today's large, constantly changing networks. Most of the dominant routing algorithms today are dynamic routing algorithms, which adjust to changing network circumstances by analysing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly. Also refer to 9.5.1 - Introducing RIP on page 183.
static and dynamic	Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.

What is a default route?

A default route is a route (also called gateway) that is used to direct packets addressed to networks not explicitly listed in the routing table. A default route is also typically used when only one specific remote network has to be reached.

What is a routing table?

The routing table is composed of a set of routes that are known to the router. It includes a list of known addresses, as well as information to get a packet one router closer to its final destination. Routing tables can be static (with routes manually entered by the network administrator) or dynamic (where routers communicate to exchange connection and route information using e.g. RIP).

9.3.2 Configuring a default route

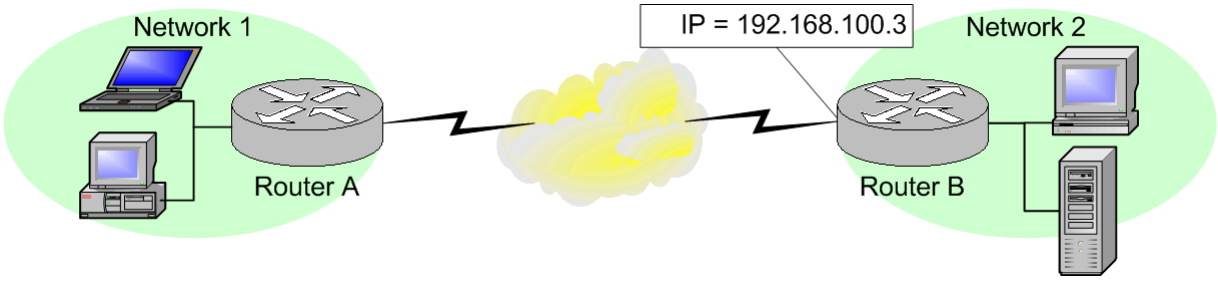
Refer to 9.3.1 - Introducing static routing on page 169 for an introduction on the default route.

To configure a default route, proceed as follows:

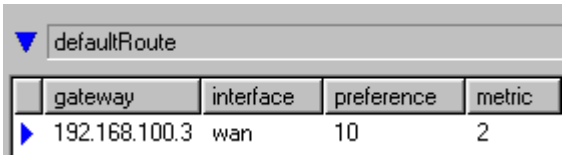
Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object and select the defaultRoute attribute.
2	Configure the elements in the defaultRoute structure. The most important elements are: • gateway. Use this element to specify the IP address of the next router that will route all packets for which no specific (static or dynamic) route exists in the routing table. • interface. Use this element to specify the interface through which the gateway can be reached. Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name). Note that this interface can also be a DLCI, PVC, tunnel, etc. Refer to telindus24xx/ip/router/defaultRoute on page 402 for more information on.

Example - configuring a default route

Suppose network 1 is connected over a network of an operator to network 2. Network 1 only needs to reach network 2. So for the router in network 1 it suffices to configure a default route towards network 2.



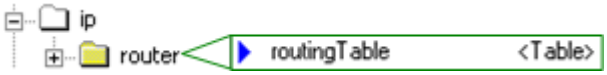
Configure the defaultRoute attribute of Router A as follows:



9.3.3 Configuring the routing table

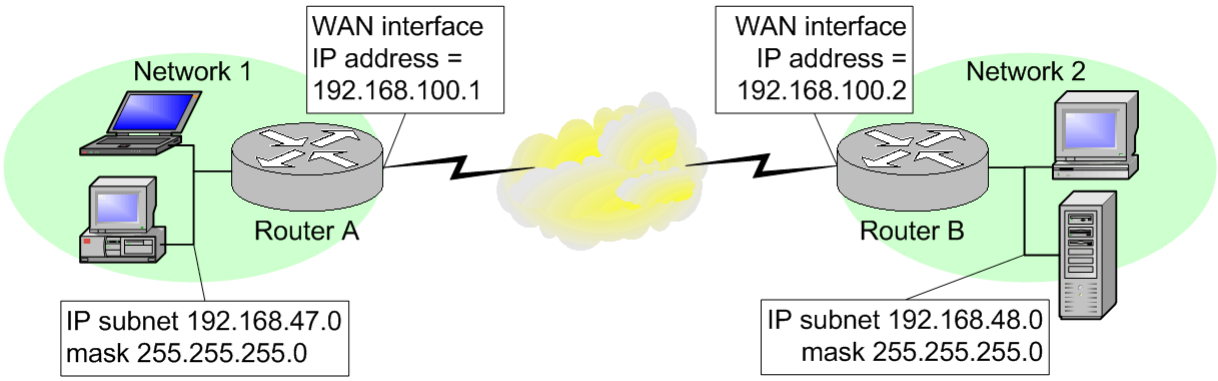
Refer to 9.3.1 - Introducing static routing on page 169 for an introduction on the routing table.

To configure the routing table, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object and select the routingTable attribute. 
2	Configure the elements in the routingTable: • network. Use this element to specify the IP address of the destination network. • mask. Use this element to specify the network mask of the destination network. • gateway. Use this element to specify the IP address of the next router on the path to the destination network. • interface. Use this element to specify the interface through which the destination network can be reached. Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name). Note that the “interface” can also be a DLCI, PVC, tunnel, etc. • preference. Use this element to set the level of importance of the route with respect to routes learnt via RIP. This element is only important when combining static routes and RIP routes. • metric. Use this element to set with how much the metric parameter of a route has to be incremented. This element is only important when combining static routes and RIP routes. Refer to telindus24xx/ip/router/routingTable on page 403 for more information.

Example - configuring a static route (WAN IP address is present)

Suppose network 1 is connected over a network of an operator to network 2. The two routers have an IP address on their WAN interface.



To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in Router A and one static route in Router B. So configure the routingTable attribute of Router A and B as follows:

Router A :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.100.2		10	2

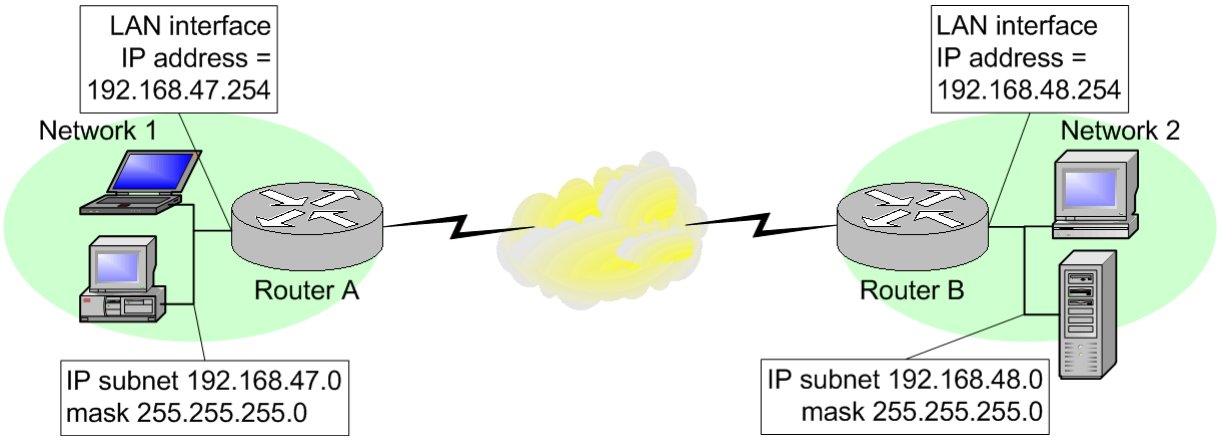
Router B :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.100.1		10	2

Example - configuring a static route (WAN IP address is not present)

Suppose network 1 is connected over a network of an operator to network 2. The two routers do not have an IP address on their WAN interface, only on their LAN interface.



To make network 192.168.48.0 reachable from network 192.168.47.0 and vice versa, you have to define one static route in Router A and one static route in Router B. So configure the routingTable attribute of Router A and B as follows:

Router A :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.48.254	wan	10	2

Router B :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.47.254	wan	10	2

9.3.4 Configuring the routing table - rules of thumb

The following are some rules when configuring the routingTable:

Rule	Description
1	As a rule of thumb, one can say that the interface name has priority over the gateway.
2	In case you enter a correct (i.e. existing) interface name and in case it refers to a … • point-to-point (PTP) interface, the route is always added to the routing table, no matter which gateway (GW) is specified. • multi-point (MP) interface, then … - the route is only added to the routing table when a local gateway is specified. - the route is not added to the routing table when no gateway is specified. - a reroute occurs when no local gateway is specified.
3	In case you enter an incorrect interface name, the route is not added to the routing table.
4	In case you enter no interface name then … • the route is added to the routing table when a local gateway is specified. • the route is not added to the routing table when no gateway is specified. • the route is not added to the routing table when the gateway lies within the configured network route. For example: network = 10.0.0.0; mask = 255.255.255.0; gateway = 10.0.0.1. • a reroute occurs when no local gateway is specified.

The following table summarises the above:

Interface name	Gateway	Result
correct	none (0.0.0.0)	• PTP: route added • MP: route not added
correct	local	route added (always)
correct	not local	• PTP: route added[1] • MP: rerouted
incorrect	-	route not added
no name	local for an interface	routed added
no name	not local for an interface Exception: • GW = none (0.0.0.0) • GW lies in configured network route	rerouted to gateway • route not added • route not added

1. In the routingTable status, the configured gateway will appear but for the routing itself the gateway is ignored.

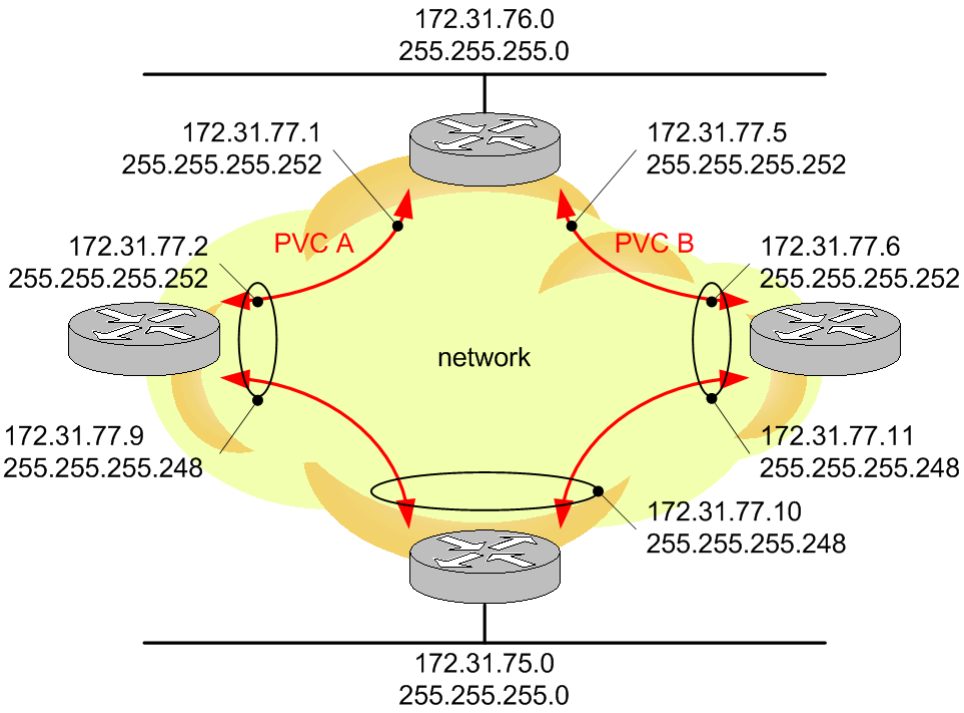
9.3.5 The rerouting principle

What is the rerouting principle?

If the gateway of a route does not belong to the subnet of an interface, then the Telindus 2400 adds a special route. Then a second route look-up occurs, this time using the gateway field of the route. This can be used as a back-up functionality as shown below.

Example

Suppose you have the following set-up:



In the routing table, the following routes are defined:

- network 172.31.75.0 is reachable via 172.31.77.10
- 172.31.77.10 is reachable via PVC A (172.31.77.2)
- 172.31.77.10 is also reachable via PVC B (172.31.77.6)

routingTable

	network	mask	gateway	interface	preference	metric
1	172.31.75.0	255.255.255.0	172.31.77.10		10	2
2	172.31.77.10	255.255.255.248	172.31.77.2	wan	10	2
3	172.31.77.10	255.255.255.248	172.31.77.6	wan	10	2

Now in order to reach network 172.31.75.0, PVC A is used. However, when PVC A goes down, the Telindus 2400 automatically uses PVC B in order to reach network 172.31.75.0. I.e. it automatically “reroutes” and this without the need of a routing protocol.

Important remarks

- This only works for the entries of the routing table, *not* for the default gateway.
- This type of route is always up.
- In the status information, the interface element of such a route displays internal.

9.4 Configuring policy based routing

This section introduces the policy based routing and gives a short description of the attributes you can use to configure policy based routing.

The following gives an overview of this section:

- 9.4.1 - Introducing policy based routing on page 177
- 9.4.2 - Setting up policy based routing on page 178

9.4.1 Introducing policy based routing

What is policy based routing?

Normal routing is based on the destination IP address. Policy based routing offers the possibility to define different routing entries based on additional information. Traffic is routed to a certain interface or gateway based on e.g. the source IP address, the IP protocol, etc.

9.4.2 Setting up policy based routing

Refer to 9.4.1 - Introducing policy based routing on page 177 for an introduction.

Configuring policy based routing basically involves the following:

- Configure a traffic policy. Based on the traffic policy criteria the data is redirected to a certain interface.
- Create a route that “points” to the traffic policy.

So to configure policy based routing, proceed as follows:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Create a traffic policy for policy based routing purposes

In the Telindus 2400 containment tree, go to the profiles/policy/traffic object and add an ipTrafficPolicy[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56).

E.g. ipTrafficPolicy[myIpPol]</td></tr>
<tr><td>2</td><td>Select a traffic policy method. Do this using the method attribute in the ipTrafficPolicy[ ] object you added in step 1.

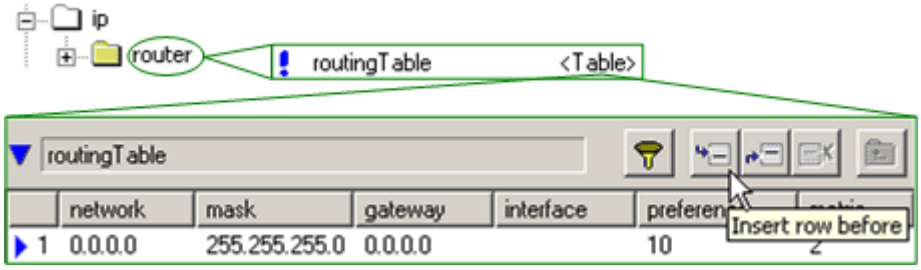
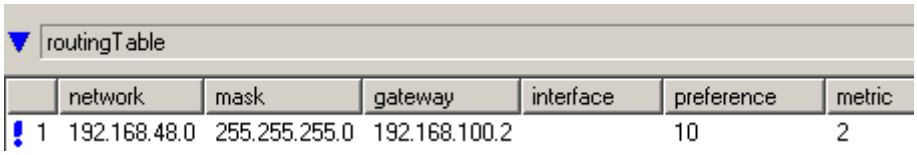
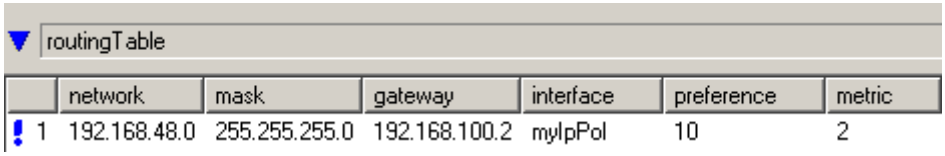
In case of policy based routing, you can only use trafficShaping or tosMapped, not tosDiffServ.</td></tr>
<tr><td>3</td><td>Configure the policy criteria for the traffic policy method you selected in step 2.

<table>
<tr><th>If you choose the method …</th><th>then use the following attribute in the ipTrafficPolicy[ ] object to configure the policy criteria:</th></tr>
<tr><td>trafficShaping,</td><td>trafficShaping.

So using the elements in this table you can route traffic based on IP source and destination address, TOS values, IP protocol, etc. The interface and gateway elements in this table determine to which interface or gateway the traffic is routed.</td></tr>
<tr><td>tosMapped,</td><td>tos2QueueMapping.

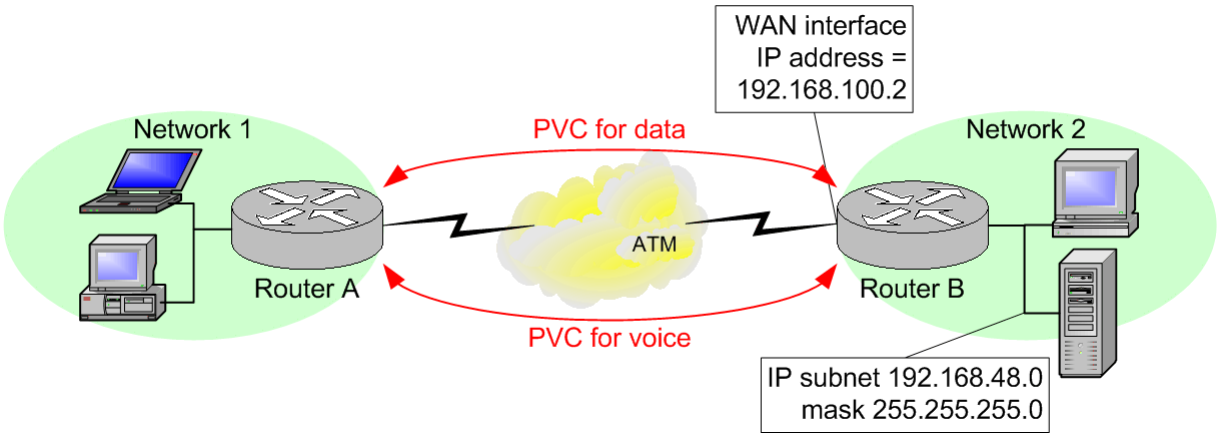
So using the elements in this table you can route traffic based on TOS values. The interface and gateway elements in this table determine to which interface or gateway the traffic is routed.</td></tr>
</table>

For more information on these attributes, refer to …
• telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping on page 382.
• telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping on page 387.</td></tr>
</table>

Step	Action
4	**Create a route that "points" to the traffic policy** In the Telindus 2400 containment tree, go to the ip/router object, select the routingTable attribute and add an entry to this table. 
5	In this entry, configure the elements network, mask, gateway, preference and metric as needed. Refer to 9.3.3 - Configuring the routing table on page 171. For example: 
6	Now you still have to let this entry "point" to the traffic policy you created earlier. Do this by entering the index name of the ipTrafficPolicy[ ] object you added in step 1 as value for the interface element. In our example the ipTrafficPolicy[ ] object is called ipTrafficPolicy[myIpPol]. So enter myIpPol as value for the interface element. 

Example - configuring policy based routing

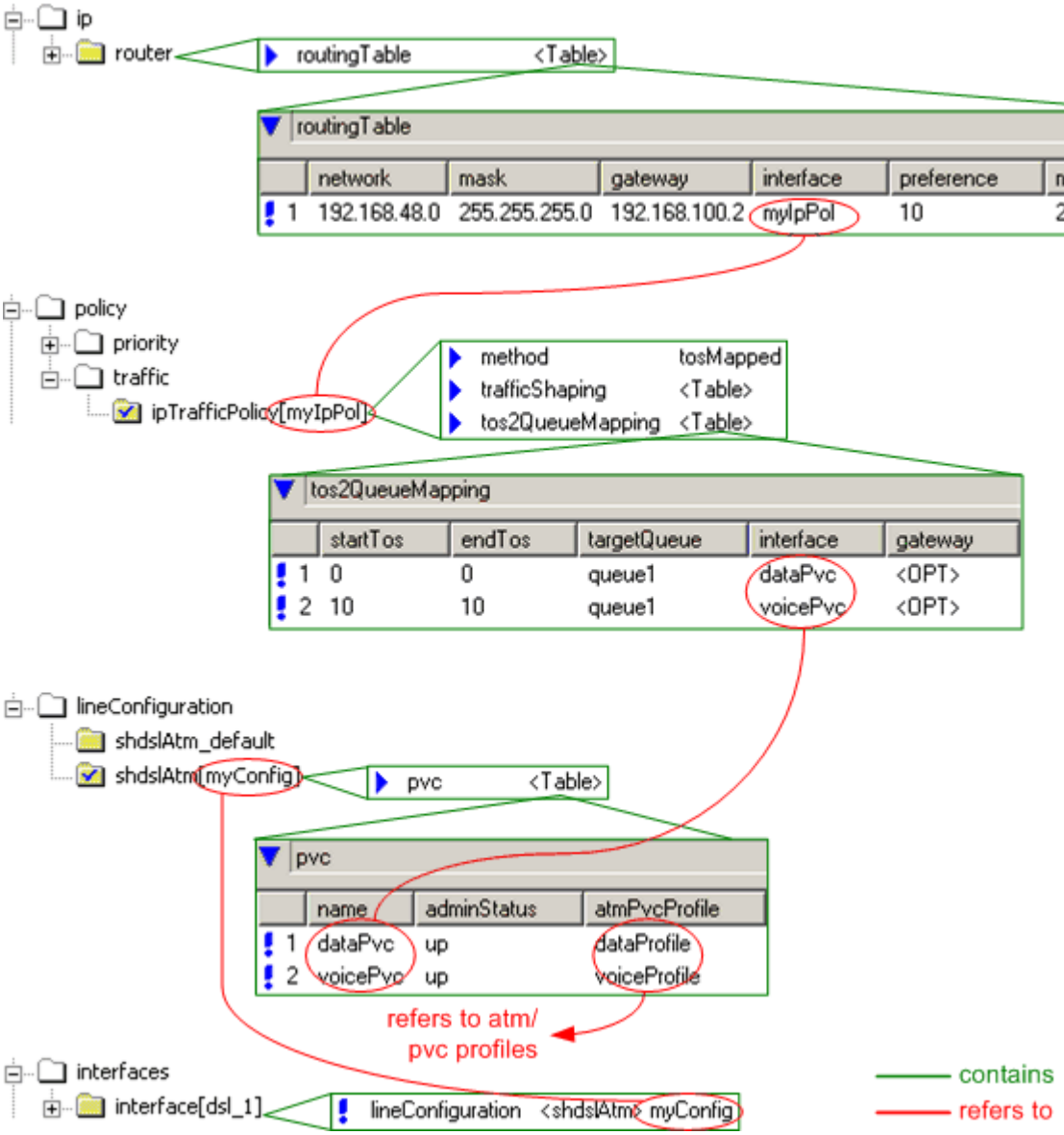
Suppose you have two networks which are interconnected via an xDSL link over an ATM network. Network 1 carries a mix of data and voice traffic. The traffic on this network is differentiated by setting the Type Of Service (TOS) values in the IP packet headers (data = 0, voice = 10). When the traffic is routed from network 1 to network 2 you want that the data traffic and the voice traffic each go over a separate PVC on xDSL line 1.



Sketched in broad outlines, this is how you configure the above:

Step	Action
1	Create and apply the necessary profiles to configure the xDSL line and to set up the ATM PVCs. For example: • Define one ATM PVC that will carry the data traffic, e.g. pvc/name = dataPvc. • Define another ATM PVC that will carry the voice traffic, e.g. pvc/name = voicePvc. • Activate these ATM PVCs on xDSL line 1. Since this is not the main subject of this example, refer for more information on creating ATM PVCs on xDSL lines to 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126.
2	Create and configure an IP traffic policy for policy based routing purposes. For example: • Create an ipTrafficPolicy[myIpPol] object. • Set the method attribute to tosMapped. • In the tos2QueueMapping structure, create two entries and define the startTos, endTos and interface elements of each entry in such a way that the data traffic and the voice traffic each go over a separate PVC.
3	Create a route that “points” to this traffic policy. For example: Create an entry in the routingTable attribute in which you specify that traffic destined for network 192.168.48.0 has to be sent to the IP traffic policy you created earlier.

The following figure shows how to configure policy based routing:



9.5 Configuring the Routing Information Protocol

This section introduces the Routing Information Protocol (RIP) and gives a short description of the attributes you can use to configure RIP.

The following gives an overview of this section:

- 9.5.1 - Introducing RIP on page 183
- 9.5.2 - Enabling RIP on an interface on page 184
- 9.5.3 - Explaining the rip structure on page 186
- 9.5.4 - Enabling RIP authentication on an interface on page 190

9.5.1 Introducing RIP

What is RIP?

The Routing Information Protocol (RIP) is a protocol that routers use to exchange dynamic routing information. RIP can be enabled or disabled per interface.

There are two main RIP modes:

RIP mode	Description
passive	Received RIP updates are parsed, but no RIP updates are transmitted.
active	RIP updates are transmitted and received.

How does RIP work?

When RIP is enabled, the Telindus 2400 advertises every 30 seconds its routing information to adjacent routers. It also receives the routing information from the adjacent routers. With this information it adapts its routing table dynamically. If after 180 seconds no information about a certain route has been received, then this route is declared *down*. If after an additional 120 seconds (i.e. 300 seconds in total) still no information about the route has been received, then this route is deleted from the routing table.

RIP support

The Telindus 2400 supports RIP protocol version 1, 1-compatible and 2. RIP version 1 is a very common routing protocol. Version 2 includes extra features like variable subnet masks and authentication. Check which RIP version is used by the other routers in the network.

Currently, the RIPv2 routing protocol requires the use of an IP address on the WAN interface.

RIP authentication

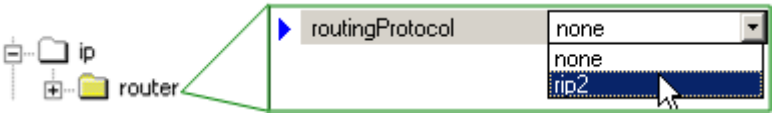
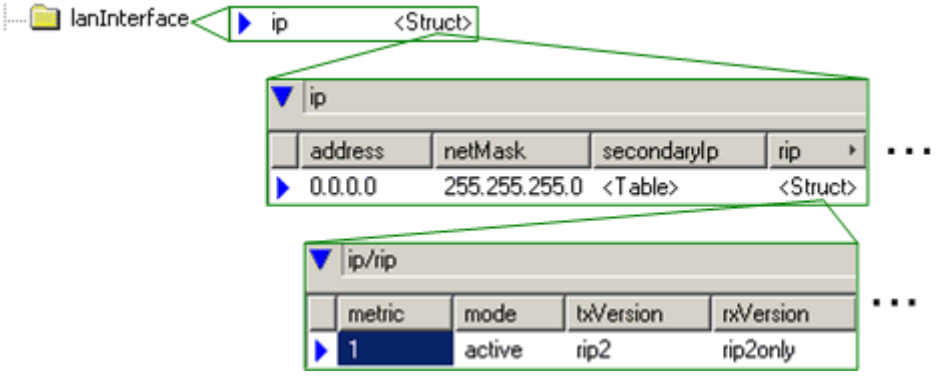
For security reasons the RIP updates that are exchanged between routers can be authenticated. RIP authentication can be enabled or disabled per interface.

9.5.2 Enabling RIP on an interface

Refer to …

- 9.3.1 - Introducing static routing on page 169 for a comparison between static and dynamic (e.g. using RIP) routing.
- 9.5.1 - Introducing RIP on page 183 for an introduction on RIP.

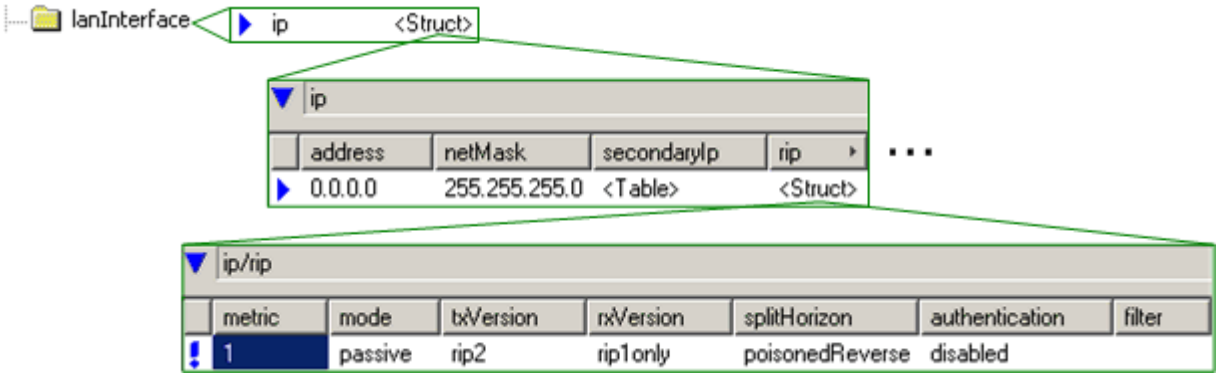
To enable dynamic routing using RIP on an IP interface, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object and set the routingProtocol attribute to rip.  This activates the general RIP process on the Telindus 2400. Now you can activate or deactivate RIP per IP interface. Note that by default RIP is activated on all IP interfaces.
2	Each IP interfaces has an ip structure. Within this ip structure you find a rip structure. Use the following elements in the rip structure to activate or deactivate RIP per IP interface: • mode. Use this element to set the transmission and/or reception of RIP updates on the interface. By default the Telindus 2400 transmits and receives RIP updates on all interfaces. • txVersion. Use this element to set the version of the RIP updates that are transmitted on the interface. • rxVersion. Use this element to set which version of received RIP updates is accepted on the interface. For example, the following shows the location of the rip structure on the LAN interface:  Refer to … • 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure on the different IP interfaces. The rip structure is located within the ip structure. • 9.5.3 - Explaining the rip structure on page 186 for a detailed explanation of the rip structure.

Example - configuring RIP

Suppose you want to activate RIP on the LAN interface. What is more, you want that the LAN interface does not transmit RIP updates but only parses received RIP updates (passive RIP). Furthermore, you only want to accept RIP version 1 updates on the LAN interface.

The following figure shows how to configure this:



Note that since in this example the mode element is set to passive, the txVersion element is ignored.

9.5.3 Explaining the rip structure

Because the rip structure occurs in several objects, it is described here once and referenced where necessary. The rip structure is located within the ip structure. Refer to 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure.

The rip structure contains the following elements:

Element	Description
metric	Use this element to determine with how much the Telindus 2400 increments the metric parameter of a route. Default:1 Range: 1 … 15 Routing information includes a metric parameter. Every time a router is passed, this parameter is incremented. Also the Telindus 2400 increments the metric parameter (default by 1) before it writes the route in the routing table. Hence, the metric parameter indicates for each route how many routers have to be passed before reaching the network. When several routes to a single network exist and they all have the same preference, then the route with the smallest metric parameter is chosen. However, using the metric element, you can increment the metric parameter by more than 1 (up to a maximum of 15). You could do this, for instance, to indicate that a certain interface is less desirable to route through. As a result, the Telindus 2400 adds this value to the metric parameter of every route learnt through that interface. The metric parameter is also used to represent the directly connected subnets on the LAN and WAN interfaces.
mode	Use this element to set the transmission and/or reception of RIP updates on the interface. By default the Telindus 2400 transmits and receives RIP updates on all interfaces. Default:active Range: enumerated, see below The mode element has the following values: **Value** / **Description** active — RIP updates are transmitted and received on this interface. passive — RIP updates are not transmitted on this interface, but received updates are parsed. disabled — RIP updates are nor transmitted nor received on this interface.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>txVersion</td><td>Use this element to set the version of the RIP updates that are transmitted on the interface.
Default:rip2
Range: enumerated, see below

The txVersion element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>rip1</td><td>The transmitted RIP updates are RIP version 1 updates.</td></tr>
<tr><td>rip2</td><td>The transmitted RIP updates are RIP version 2 updates.</td></tr>
<tr><td>rip1-compatible</td><td>The contents of the RIP update packet is a RIP version 2 packet, but it is encapsulated as a RIP version 1 packet. This allows some older implementations of RIP 1 to be interoperable with RIP 2.</td></tr>
</table></td></tr>
<tr><td>rxVersion</td><td>Use this element to set which version of received RIP updates is accepted on the interface.
Default:rip2only
Range: enumerated, see below

The rxVersion element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>rip1only</td><td>Only RIP version 1 received RIP updates are accepted.</td></tr>
<tr><td>rip2only</td><td>Only RIP version 2 received RIP updates are accepted.</td></tr>
<tr><td>rip1&2</td><td>Both RIP version 1 and 2 received RIP updates are accepted.</td></tr>
</table>

If you want to accept RIP1-compatible updates on the interface, then set the rxVersion attribute to rip1&2.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>splitHorizon</td><td>Use this element to enable or disable split horizon operation.
Default:poisonedReverse
Range: enumerated, see below

The splitHorizon element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Split horizon is disabled.</td></tr>
<tr><td>enabled</td><td>Split horizon is enabled.

Split horizon operation prevents that routing information exits the interface through which the information was received in the first place. This optimises communications among multiple routers, particularly when links are broken. It also prevents routing loops.</td></tr>
<tr><td>poisonedReverse</td><td>Poisoned reverse split horizon is used.

Whereas “simple” split horizon simply omits the routes learned from one neighbour in updates sent to that neighbour, poisoned reverse split horizon includes such routes in updates but sets their metrics to infinity.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>authentication</td><td>
Use this element to enable or disable RIP authentication.
Default:disabled
Range: enumerated, see below

Refer to 9.5.4 - Enabling RIP authentication on an interface on page 190 for more information on RIP authentication.

The authentication element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>No authentication is used.</td></tr>
<tr><td>text</td><td>The authentication secret is exchanged in clear text.</td></tr>
<tr><td>md5</td><td>Instead of sending the authentication secret together with the RIP updates, it is hashed together with the routing information into a unique value. This authentication is the most secure. This because it provides also protection against tampering with the contents of a packet: both an incorrect password and modified routing information result in different hash values.</td></tr>
</table>

Remarks

• If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
• If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
• If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.
</td></tr>
<tr><td>filter</td><td>
Use this element to apply a filter on the RIP updates on the interface.
Default:<empty>
Range: 0 … 24 characters

Do this by entering the index name of the filter you want to use. You can create the filter itself by adding a routingFilter object under the router object and by configuring the attributes in this object.

Example

If you created a routingFilter object with index name my_filter (i.e. routingFilter[my_filter]) and you want to apply this filter here, then enter the index name as value for the filter element.

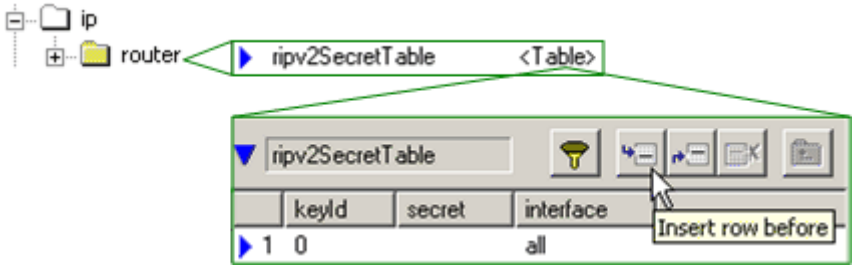
Refer to …

• 4.4 - Adding an object to the containment tree on page 56 for more information on adding objects.
• 13.12.5 - Routing filter configuration attributes on page 443 for more information on RIP filtering.
</td></tr>
</table>

9.5.4 Enabling RIP authentication on an interface

Refer to 9.5.1 - Introducing RIP on page 183 for an introduction on RIP authentication.

To enable RIP authentication on a certain interface, proceed as follows:

Step	Action
1	In the rip structure, set the authentication element to … • text. RIP authentication is enabled and the authentication secret is sent along with the RIP updates in clear text. • md5. RIP authentication is enabled and the authentication secret is hashed together with the routing information into a unique value. Refer to 9.5.3 - Explaining the rip structure on page 186.
2	In the Telindus 2400 containment tree, go to the ip/router object, select the ripv2SecretTable attribute and add one or more entries to this table. 
3	Configure the elements of an entry in the ripv2SecretTable attribute: • keyId. Use this element to set a unique identifier for each secret. • secret. Use this element to define the secret. This secret is sent with the RIP updates on the specified interface. It is also used to authenticate incoming RIP updates. • interface. Use this element to specify on which interface the secret is used. Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name). Note that the “interface” can also be a DLCI, PVC, tunnel, etc. Entering the string “all” (default) means the secret is used on all the interfaces. Refer to telindus24xx/ip/router/ripv2SecretTable on page 407 for more information.

9.6 Configuring address translation

This section introduces the Network Address Translation (NAT) and Port Address Translation (PAT) and gives a short description of the attributes you can use to configure NAT and PAT. It also contains a table that helps you to determine which translation method meets your requirements.

The following gives an overview of this section:

- 9.6.1 - Introducing address translation on page 192
- 9.6.2 - When use NAT and/or PAT on page 193
- 9.6.3 - Enabling PAT on an interface on page 194
- 9.6.4 - How does PAT work? on page 196
- 9.6.5 - PAT limitations and work-arounds on page 199
- 9.6.6 - Enabling NAT on an interface on page 200
- 9.6.7 - How does NAT work? on page 202
- 9.6.8 - Combining PAT and NAT on page 204
- 9.6.9 - Easy NAT on PPP on page 204

9.6.1 Introducing address translation

What is address translation?

Address translation is used to translate private IP addresses into official IP addresses. This is also known as IP masquerading.

Why use address translation?

Each device connected to the Internet must have an *official* (i.e. unique) IP address. The success of the Internet has caused a lack of these official IP addresses. As a result, your Internet Service Provider (ISP) may offer you only one or a small number of official IP addresses.

If the number of IP devices on your local network is larger than the number of official IP addresses, you can assign test or *private* IP addresses to your local network. In that case, you have to configure your access router to translate IP addresses using NAT or PAT.

Even when there are sufficient official IP addresses available, you may still choose to use NAT e.g. for preserving previously assigned test addresses to all the devices on your local network.

What is NAT?

Network Address Translation (NAT) is an Internet standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic (private IP addresses) and a second set of addresses for external traffic (official IP addresses). The access router (located where the LAN meets the Internet) makes all necessary IP address translations. This is a dynamic process.

NAT serves three main purposes:

- Provides a type of firewall by hiding internal IP addresses.
- Enables a company to use more internal IP addresses. Since these are used internally only, there is no possibility of conflict with IP addresses used by other companies and organizations.
- Allows a company to combine multiple ISDN connections into a single Internet connection.

The number of simultaneous users with Internet access is limited to the number of official IP addresses.

What is PAT?

Port Address Translation (PAT) is a type of Network Address Translation. During PAT, each computer on LAN is translated to the same IP address, but with a different port number assignment.

Only outgoing TCP sessions are supported.

Private IP address range

The international authority IANA assigns the official (also called global) IP addresses. It has also defined 3 ranges of IP addresses for private use. This means that you can use these addresses without registration on your internal network, as long as you are not connected to the Internet.

Private IP address range	Remarks
10.0.0.0 - 10.255.255.255	1 class A network
172.16.0.0 - 172.31.255.255	16 class B networks
192.168.0.0 - 192.168.255.255	256 class C networks

You can define (sub-)networks in these ranges for your *private IP addresses*.

9.6.2 When use NAT and/or PAT

Refer to 9.6.1 - Introducing address translation on page 192 for an introduction on NAT and PAT authentication.

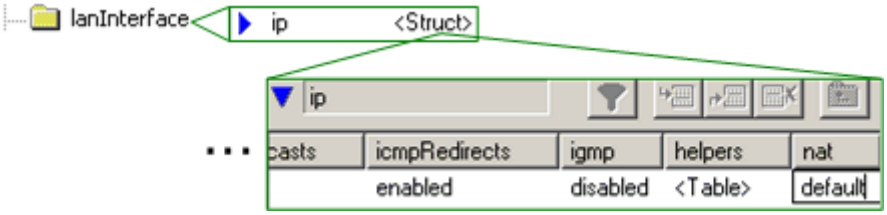
Check in the next table whether you need NAT and/or PAT:

No. of official IP addresses	No. of devices on local network	Use NAT of PAT?	Refer to …
1	more than 1	Use PAT.	9.6.3 - Enabling PAT on an interface on page 194
k (> 1)	more than k	Use NAT in combination with PAT.	9.6.8 - Combining PAT and NAT on page 204
at least k	k (≥ 1)	1. No translation needed. 2. If you want translation, use NAT.	1. Skip this section. 2. 9.6.6 - Enabling NAT on an interface on page 200

9.6.3 Enabling PAT on an interface

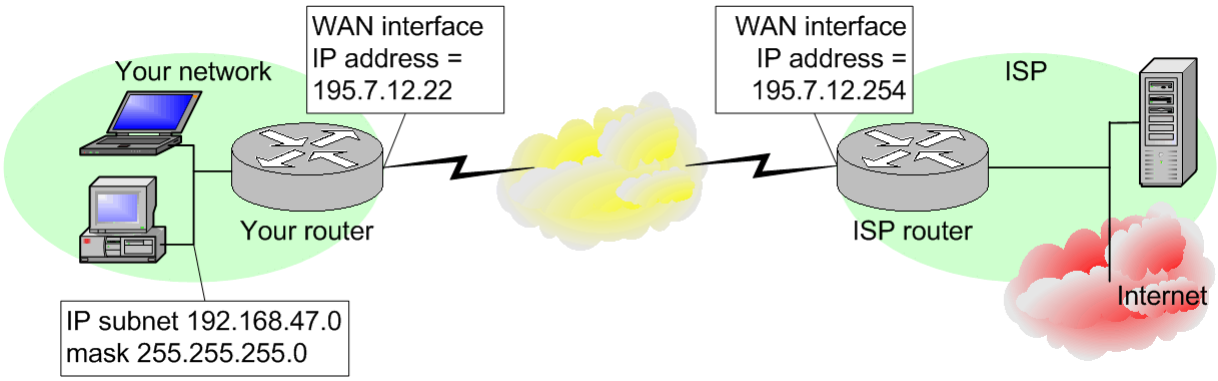
Refer to 9.6.1 - Introducing address translation on page 192 for an introduction on PAT.

To enable PAT on a certain interface, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router/defaultNat object. In this object, configure the patAddress attribute. Use this attribute to enter the official IP address that has to be used for the Port Address Translation. Entering an address different from the default value 0.0.0.0 automatically enables the general PAT process. Now you can activate or deactivate PAT per IP interface. Note that by default PAT is deactivated on all IP interfaces.
2	In the ip/router/defaultNat object, configure the gateway attribute. Use this attribute to define the gateway addresses from routes on which PAT should be applied. If you do not configure the gateway attribute, then the router/defaultRoute attribute is taken as only gateway addresses.
3	Each IP interfaces has an ip structure. Use the following element in the ip structure to activate or deactivate PAT per IP interface: • nat. Use this element to enable address translation on the interface. Do this by entering the string “default“ as nat element value. By doing so, the settings are applied as defined in the router/defaultNat object. For example, the following shows the location of the ip structure on the LAN interface:  Refer to 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure on the different IP interfaces.

Example - configuring PAT

Suppose your network is connected over a network of an operator to an Internet Service Provider (ISP). You received only one single official IP address from you ISP, being 195.7.12.22.



The following shows how to enable PAT:

- In the ip/router/defaultNat object, set the patAddress attribute to 195.7.12.22. In that case, the PAT address is the same as the IP address that is used on the WAN interface.
- In the ip/router/defaultNat object, set the gateway attribute to 195.7.12.254. If, however, you already defined the router/defaultRoute attribute to be 195.7.12.254, then you can leave the gateway attribute empty. This because if the gateway attribute is empty, then the defaultRoute attribute is taken as only gateway addresses.
- In the ip structure of the WAN interface, type the string “default” as value of the nat element.

9.6.4 How does PAT work?

Again consider the network topology as depicted in 9.6.3 - Enabling PAT on an interface on page 194.

The following two paragraphs explain how the Telindus 2400 treats the outgoing and incoming traffic when PAT is applied:

- Outgoing traffic (to the Internet) on page 196.
- Incoming traffic (from the Internet) on page 198.

Outgoing traffic (to the Internet)

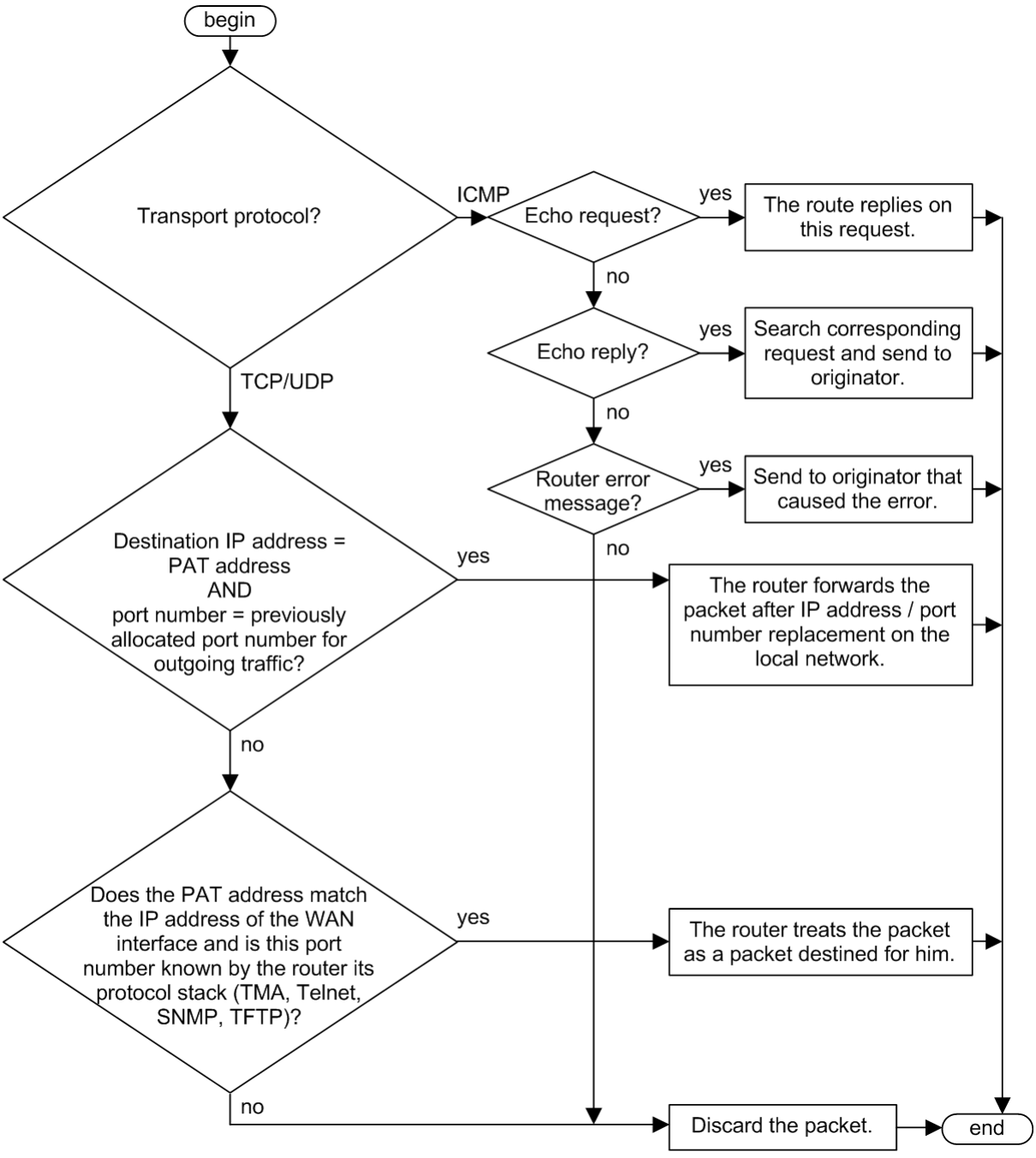
The Telindus 2400 replaces the source address by its PAT address in all the traffic coming from the local network and destined for the Internet. Depending on the IP transport protocol and the number of simultaneous users accessing the Internet, the Telindus 2400 takes different actions:

Protocol		
TCP	**Description**	This is a connection-oriented protocol: two devices communicating with the TCP protocol build a session before exchanging user data. When they have finished exchanging user data, the session is closed. Examples of such applications are Telnet, HTTP and FTP. The TCP header contains a *port* field indicating the higher-layer protocol.
	Action	When a session is started, a specific port number is assigned to this session. All traffic from this session is assigned this specific port number. The specific port number is freed within 5 minutes after the TCP session is closed (i.e. after TCP Reset or TCP Finish is seen). If the session has not been properly closed, the port number is freed 24 hours after the last session traffic. This time is configurable (refer to telindus24xx/ip/router/defaultNat/tcpSocketTimeOut on page 429).
UDP	**Description**	This is a connection-less protocol: user data can be sent without first building a session. Examples of such applications are SNMP and TFTP. Although TFTP is session-oriented, it builds the session at a higher level and uses UDP for its simplicity as transport protocol. The UDP header contains a *port* field indicating the higher-layer protocol.
	Action	The source port number is replaced by a specific port number. All traffic from this source IP address / port number pair is assigned this specific port number. If there is no traffic for 5 to 10 minutes, the specific port number is freed. If the session has not been properly closed, the port number is freed 3 minutes after the last session traffic. This time is configurable (refer to telindus24xx/ip/router/defaultNat/udpSocketTimeOut on page 429).

Protocol		
ICMP	**Description**	This is a connection-less protocol: user data can be sent without first building a session. An example of such an application is ping. These protocols do not have port numbers.
	Action	Each ICMP packet is forwarded towards the Internet. Each ICMP packet is considered as a new session. If there is no traffic for 5 to 10 minutes, the session is closed. The fact that it is possible to open a total of 2048 simultaneous sessions and that each ICMP packet is considered as a new session, implies that for instance a continuous series of ping requests at a rate of one per second will allocate between 300 and 600 sessions.

Incoming traffic (from the Internet)

Suppose the WAN IP network depicted in 9.6.3 - Enabling PAT on an interface on page 194 works in numbered mode[1]. The incoming traffic from the Internet may be destined either for the local network, or for the router itself. The router treats incoming traffic on the PAT address as follows:


begin
Transport protocol?
ICMP
Echo request?
yes
The route replies on this request.
no
Echo reply?
yes
Search corresponding request and send to originator.
no
Router error message?
yes
Send to originator that caused the error.
no
TCP/UDP
Destination IP address = PAT address AND port number = previously allocated port number for outgoing traffic?
yes
The router forwards the packet after IP address / port number replacement on the local network.
no
Does the PAT address match the IP address of the WAN interface and is this port number known by the router its protocol stack (TMA, Telnet, SNMP, TFTP)?
yes
The router treats the packet as a packet destined for him.
no
Discard the packet.
end

1. Numbered mode means that each WAN interface has an IP address. In that case, you need the single official IP address for your WAN interface.

9.6.5 PAT limitations and work-arounds

PAT limitations

Port Address Translation has some limitations:

- Some TCP or UDP applications do not support port translation.
- Only outgoing sessions are supported. This implies that you can not access servers on your local network over the Internet.
- Limited ICMP support.

PAT limitations work-arounds

Use the following attributes to partly overcome the PAT limitations:

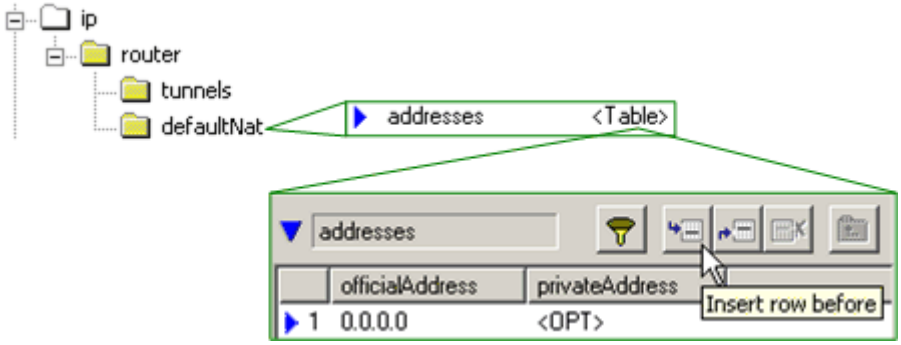
Attribute	Description
portTranslations	You can find this attribute in the ip/router/defaultNat object. Use this attribute to define specific port number ranges that should not be translated when using PAT. Refer to telindus24xx/ip/router/defaultNat/portTranslations on page 427. **Example - configuring the portTranslations table** TMA is an example of an application that does not support port translation. If you want to make TMA connections from your local network to the outside world, you have to list TMA port number 1728 in this table. However, keep in mind that even then it is still not possible to have two simultaneous TMA sessions to the same outside world address. portTranslations protocol / startPort / endPort / action 1 udp 1728 <Opt> no translation 2 udp 2000 3000 deny If you do not want that UDP packets with port numbers in the range 2000 up to 3000 are sent to the outside world, then you also have to include those in the table.
servicesAvailable	You can find this attribute in the ip/router/defaultNat object. Use this attribute to define specific port number ranges for incoming Internet traffic that should not be translated when using PAT. Instead it is sent to the corresponding private IP address. Refer to telindus24xx/ip/router/defaultNat/servicesAvailable on page 428. **Example - configuring the servicesAvailable table** In this example, a web server with address 192.168.47.250 on the local network is accessible from the Internet although it has no official IP address. servicesAvailable protocol / startPort / endPort / serverAddress 1 tcp 80 <Opt> 192.168.47.250

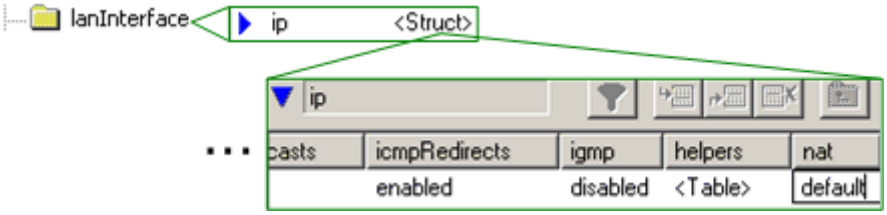
9.6.6 Enabling NAT on an interface

Refer to 9.6.1 - Introducing address translation on page 192 for an introduction on NAT.

Despite the work-arounds offered by the previous two PAT configuration attributes to overcome the limitations of PAT (refer to 9.6.5 - PAT limitations and work-arounds on page 199), there are situations where PAT is inadequate. For example, it is not possible to have several web servers on your local network. It is also impossible to run an application with fixed source port numbers on several local devices that are connected simultaneously to a single Internet device. This can only be solved by using several official IP addresses: Network Address Translation.

To enable NAT on a certain interface, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router/defaultNat object, select the addresses attribute and add one or more entries to this table.  Use this attribute to enter all the official IP addresses that have to be used for Network Address Translation. Entering an address in the addresses table automatically enables the general NAT process. Now you can activate or deactivate NAT per IP interface. Note that by default NAT is deactivated on all IP interfaces.
2	Configure the elements of the addresses table: • officialAddress. Use this element to set the official IP address. These addresses are used in the reverse order as they appear in the list. • privateAddress. Use this element to set the private IP address, i.e. to permanently assign an official IP address to a private address.
3	In the ip/router/defaultNat object, configure the gateway attribute. Use this attribute to define the gateway addresses from routes on which NAT should be applied. If you do not configure the gateway attribute, then the router/defaultRoute attribute is taken as only gateway addresses.

Step	Action
4	Each IP interfaces has an ip structure. Use the following element in the ip structure to activate or deactivate NAT per IP interface: • nat. Use this element to enable address translation on the interface. Do this by entering the string "default" as nat element value. By doing so, the settings are applied as defined in the router/defaultNat object. For example, the following shows the location of the ip structure on the LAN interface:  Refer to 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure on the different IP interfaces.

Important remark - using NAT on the LAN interface

Consider the following configuration:

- telindus24xx/lanInterface/ip/address = 195.7.12.22
- telindus24xx/router/defaultNat/addresses = { officialAddress = 195.7.12.22; privateAddress = <opt> }
- telindus24xx/wanInterface/ppp/ip/address = 2.2.2.2

The above means that NAT is used on the LAN interface and the router uses the address 195.7.12.22 as official IP address.

The problem that arises here is that the router can no longer be managed via the LAN interface using the management tool (TMA, Telnet, etc.). This because the NAT route has priority over the LAN route and, because it is a NAT address, the router does not accept incoming traffic on the address 195.7.12.22.

The solution is to add the WAN IP address to the addresses table as private address: telindus24xx/router/addresses = { officialAddress = 195.7.12.22; privateAddress = 2.2.2.2 }. In that case, the management tool "service" runs on the WAN IP address. This means however, that the WAN has to be up.

9.6.7 How does NAT work?

Dynamically assigning official IP address

If a local station sends data to the Internet for the first time, NAT looks for an unused official IP address. It assigns this official IP address to the local station. The amount of local stations that can have simultaneous Internet access equals the amount of NAT addresses you defined. If all sessions between a local station and the Internet have been closed by the application (in case of TCP) or because of time-outs, then the previously assigned official IP address is freed for another local station.

Statically assigning official IP address

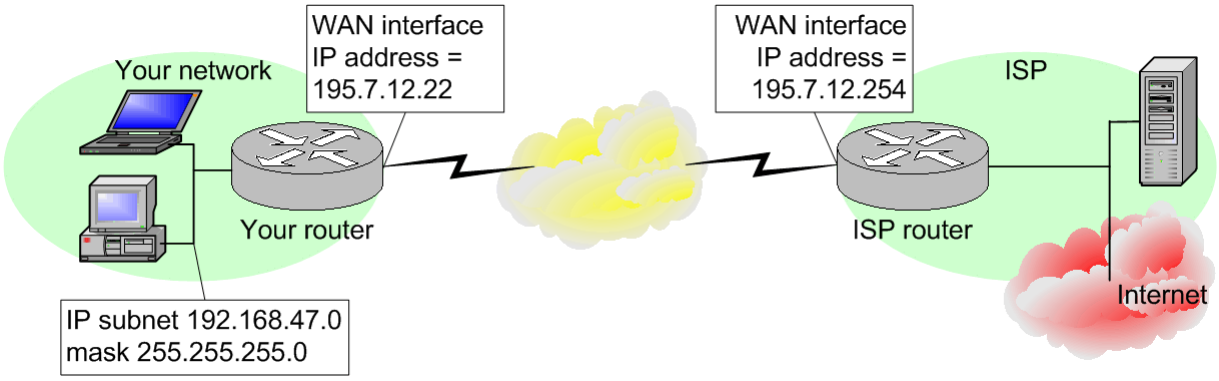
Optionally, the NAT address entry may contain a corresponding private IP address. This allows to permanently assign an official IP address to a local station. This is useful for stations or servers that should have Internet access at all times. Another example of permanently assigned official IP addresses is a network where only a limited number of users has Internet access.

Incoming traffic on an official IP address

NAT only converts IP addresses and thus allows traffic in both directions. However, incoming traffic on one of the official IP addresses can only be forwarded to the local network if a corresponding private IP address has been configured.

Example - configuring NAT

Suppose your network is connected over a network of an operator to an Internet Service Provider (ISP). You received 4 official IP address from you ISP, being 195.7.12.21 up to 195.7.12.24. You want to assign one of these official addresses permanently to a web server which has private address 192.168.47.250. All other official addresses have to be assigned dynamically.



The following shows how to enable NAT:

- In the ip/router/defaultNat object, configure the addresses attribute as follows:

addresses

	officialAddress	privateAddress
1	195.7.12.21	192.168.47.250
2	195.7.12.22	<OPT>
3	195.7.12.23	<OPT>
4	195.7.12.24	<OPT>

- In the ip/router/defaultNat object, set the gateway attribute to 195.7.12.254. If, however, you already defined the router/defaultRoute attribute to be 195.7.12.254, then you can leave the gateway attribute empty. This because if the gateway attribute is empty, then the defaultRoute attribute is taken as only gateway addresses.
- In the ip structure of the WAN interface, type the string “default” as value of the nat element.

9.6.8 Combining PAT and NAT

It is possible to use a combination of PAT and NAT. In that case the router first assigns NAT addresses until they are all used. Then it uses PAT addresses for further translations.

Make sure the PAT address does not appear in the NAT address table.

9.6.9 Easy NAT on PPP

What is easy NAT on PPP?

Easy NAT on PPP means that in a typical client / ISP setup NAT will automatically be enabled without the need to specifically configure NAT.

A typical client / ISP setup would be, for example, a Telindus 1421 SHDSL Router on the client side and a Telindus 2400 on the ISP side connected over an SHDSL line.

What are the conditions for easy NAT on PPP?

The conditions for easy NAT on PPP are:

- A PPP (or PPPoA) connection between ISP and client.
- PPP interface on ISP router:
  - The mode is routing.
  - A local IP address may be configured, or it may be coming from the LAN (unnumbered).
  - A remote IP address is imposed on the client router.
  - NAT is disabled.
- PPP interface on client router:
  - The mode is routing.
  - No local nor remote IP address is configured.
  - NAT is enabled (a reference is made to the defaultNat object).
- The defaultNat object on the client router:
  - No PAT address is configured.
  - No NAT address(es) is (are) configured.

What does easy NAT on PPP?

Once the conditions as stated above are met, the following happens:

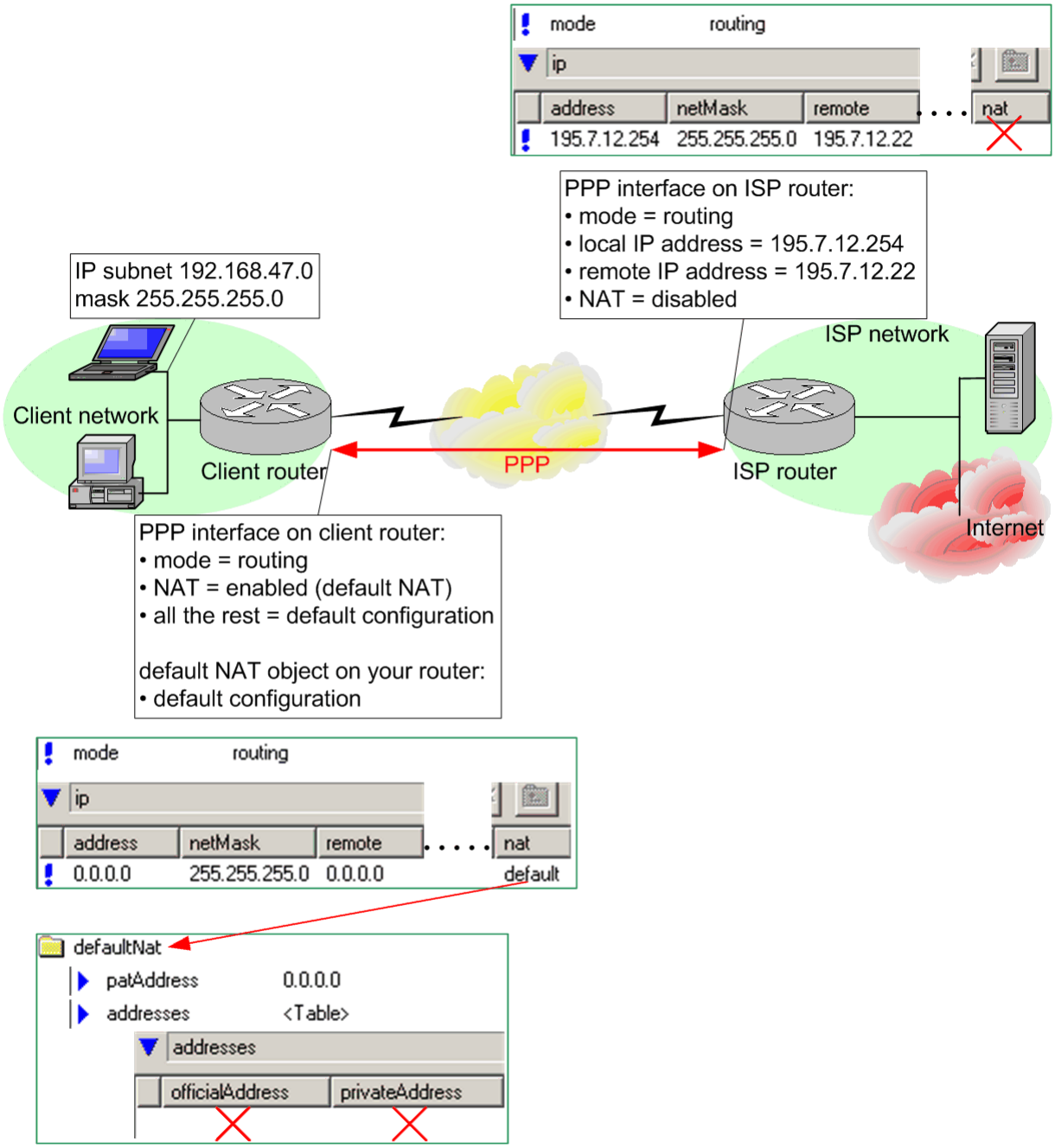
- The client router learns the local and remote IP address of the PPP link from the ISP router.
- The client router adds a route towards the ISP router.
- The client router enables NAT on the PPP interface.

Note that in the easy NAT context the Telindus 2400 …

- can only act as the ISP router, not as the client router on its xDSL interfaces. In this case, the Telindus 1421 SHDSL Router, for example, can act as client router.
- can act as both client and ISP router on its TIM (Telindus Interface Module).

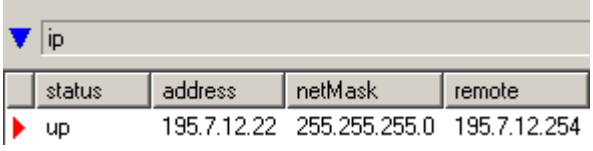
Example - easy NAT

Suppose you have the following setup:

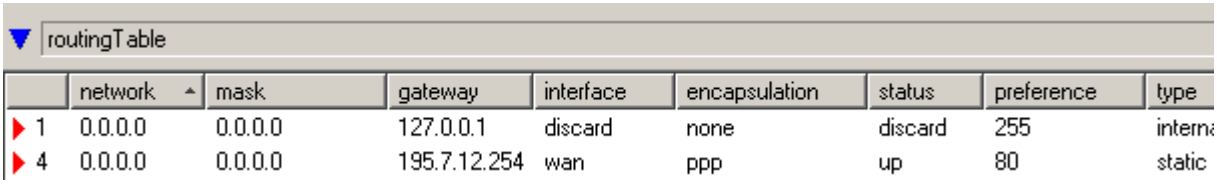


Once the PPP link is up and running, you will see that …

- the client router learns the local and remote IP address of the PPP link from the ISP router. You can check this by looking at the IP status of the PPP link:



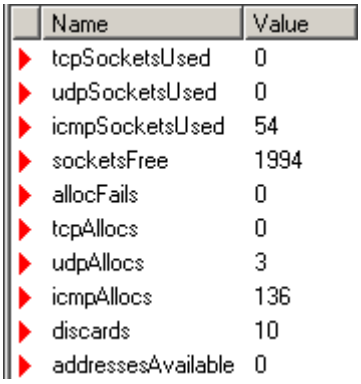
- The client router adds a route towards the ISP router. You can check this by looking at the routing table status:



routingTable

	network	mask	gateway	interface	encapsulation	status	preference	type
1	0.0.0.0	0.0.0.0	127.0.0.1	discard	none	discard	255	interna
4	0.0.0.0	0.0.0.0	195.7.12.254	wan	ppp	up	80	static

- The client router enables NAT on the PPP interface. You can check this by looking at the default NAT performance. When a connection to the ISP is active, you will see that socketsFree attribute decreases while the used sockets (xxxSocketsUsed) and allocation (xxxAllocs) attributes increase.



Name	Value
tcpSocketsUsed	0
udpSocketsUsed	0
icmpSocketsUsed	54
socketsFree	1994
allocFails	0
tcpAllocs	0
udpAllocs	3
icmpAllocs	136
discards	10
addressesAvailable	0

9.7 Configuring traffic and priority policy on the router

This section introduces traffic and priority policy and gives a short description of the attributes you can use to configure these features on the router. It also shows you the difference with the traffic policy on the bridge.

The following gives an overview of this section:

- 9.7.1 - Introducing traffic and priority policy on page 208
- 9.7.2 - Traffic and priority policy on routed and on bridged data on page 211
- 9.7.3 - How to configure a traffic and priority policy on the router? on page 212
- 9.7.4 - Creating a traffic policy on the router on page 213
- 9.7.5 - Applying a traffic policy on an interface of the router on page 215
- 9.7.6 - Creating a priority policy on page 216
- 9.7.7 - Applying a priority policy on an interface on page 218
- 9.7.8 - Configuring a traffic and priority policy on the router - an example on page 219

9.7.1 Introducing traffic and priority policy

What is traffic and priority policy?

Because of the bursty nature of voice / video / data traffic, sometimes the amount of traffic exceeds the speed of a link. At this point, the Telindus 2400 has to decide what to do with this “excess” of traffic:

- Buffer the traffic in a single queue and let the first packet in be the first packet out?
- Or put packets into different queues and service certain queues more often (also known as priority queuing)?

These questions are dealt with by the traffic and priority policy mechanisms:

- The traffic policy determines, on traffic overload conditions, how and which queues are filled with the “excess” data.
- The priority policy determines how and which queues are emptied.

What is a priority queuing?

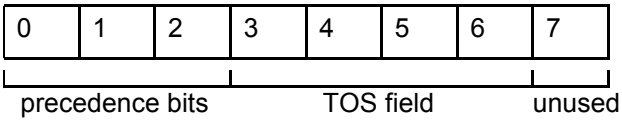
Using the traffic and priority policy features you can perform priority queuing. This allows you to define how traffic is prioritised in the network. E.g. to ensure that voice, video or other streaming media is serviced before (or after) other traffic types, to ensure that web response traffic is routed before normal web browsing traffic, etc.

Per interface (both physical and logical), there are 7 queues:

Queue	Queue type	Description
1 - 5	user configurable queue	The user can decide which data goes into which queue.
6	low delay queue	The user can decide which data goes into this queue. This queue usually is addressed more often then the user configurable queues.
7	system queue	This queue is filled with mission critical data (e.g.link monitoring messages etc.) and has priority over all other queues.

What is the TOS byte?

The Type Of Service (TOS) byte is an eight bit field in the IP header. It is structured as follows:



What is the precedence field?

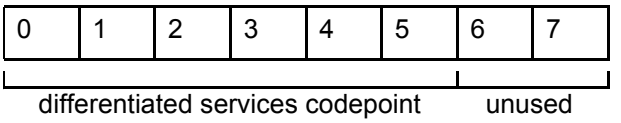
The precedence field is a three bit field in the TOS byte of the IP header (see RFC 791). Using the precedence field, a network administrator can assign values from 0 to 7 to classify and prioritise types of traffic. IP precedence is being phased out in favour of DSCP, but is supported by many applications and routers.

What is the TOS field?

The TOS field is a four bit field in the TOS byte of the IP header (see RFC 1349). It lets values from 0 to 15 be assigned to request special handling of traffic (for example, minimize delay, maximize throughput). The TOS field is being phased out in favour of DSCP.

What is DSCP or Diff-Serv?

Differentiated Services Code Point (DSCP) uses the TOS byte differently (see RFC 2474). Six bits of the TOS byte are being reallocated for use as the DSCP field, where each DSCP specifies a particular per-hop behaviour that is applied to a packet.



DSCP is not compatible with IP Precedence.

What is PHB?

A Per-Hop Behaviour (PHB) is a basic hop-by-hop resource allocation mechanism. Think of PHB as a particular forwarding behaviour that stretches across a network and that provides a particular class of service.

The Telindus 2400 features Assured Forwarding PHB (RFC 2597).

What is AF PHB?

Assured Forwarding Per-Hop Behaviour (AF PHB, see RFC 2597) defines a method for defining drop precedence. IP packets are marked with one of three possible drop precedence values. When congestion occurs, the congested DS node protects packets with a lower drop precedence value by discarding packets with a higher drop precedence value.

What is IEEE 802.1P?

The IEEE 802.1P signalling technique (also often referred to as Class Of Service, COS) is an IEEE endorsed specification for prioritising network traffic at the datalink/MAC sub-layer (layer 2).

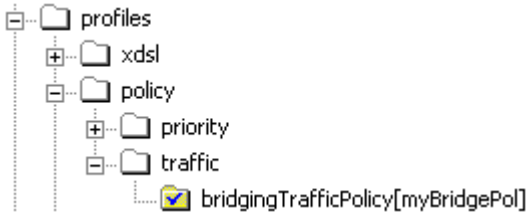
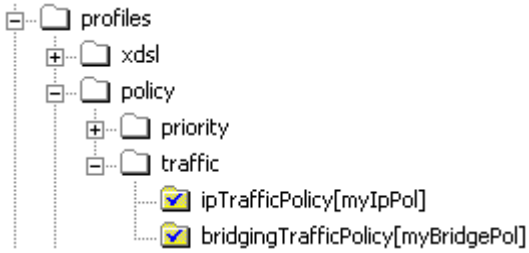
802.1P is a spin-off of the 802.1Q (VLAN tagging) standard and they work in tandem. The 802.1Q standard specifies a tag that appends to a MAC frame. The VLAN tag carries VLAN information. The VLAN tag has two parts: The VLAN ID (12-bit) and prioritisation (3-bit). The prioritisation field was never defined in the VLAN standard. The 802.1P implementation defines this prioritisation field.

9.7.2 Traffic and priority policy on routed and on bridged data

Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for an introduction.

Traffic policy on routed and on bridged data

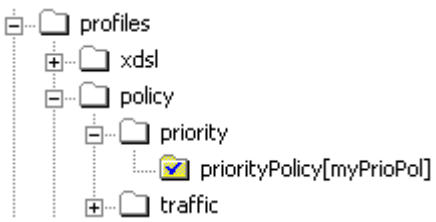
The traffic policy (i.e. the policy to fill the queues) is not the same for routed data as the one for bridged data. The following table clarifies this:

In case … is enabled,	then …
only routing	the routed data is queued using the traffic policy settings as configured in the ipTrafficPolicy[ ] object under the profiles/policy/traffic object. Refer to 9.7.4 - Creating a traffic policy on the router on page 213.
only bridging	the bridged data is queued using the traffic policy settings as configured in the bridgingTrafficPolicy[ ] object under the profiles/policy/traffic object.  Refer to 10.3.2 - Configuring a traffic policy on the bridge on page 247.
routing and bridging	• the routed data is queued using the traffic policy settings as configured in the ipTrafficPolicy[ ] object under the profiles/policy/traffic object. Refer to 9.7.4 - Creating a traffic policy on the router on page 213.  • the bridged data is queued using the traffic policy settings as configured in the bridgingTrafficPolicy[ ] object under the profiles/policy/traffic object. Refer to 10.3.2 - Configuring a traffic policy on the bridge on page 247.

Priority policy on routed and on bridged data

The priority policy (i.e. the policy to empty the queues) is the same for routed and bridged data. The queues are emptied using the priority policy settings as configured in the priorityPolicy[ ] object under the profiles/policy/priority object.

Refer to 9.7.6 - Creating a priority policy on page 216.



9.7.3 How to configure a traffic and priority policy on the router?

Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for an introduction.

To configure a traffic and priority policy for the routed data on a certain interface, proceed as follows:

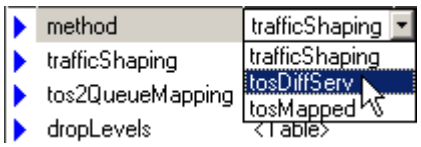
Step	Action
1	Create and configure a routing traffic policy. Refer to 9.7.4 - Creating a traffic policy on the router on page 213.
2	Apply the routing traffic policy on the desired interface. Refer to 9.7.5 - Applying a traffic policy on an interface of the router on page 215.
3	Create and configure a priority policy. Refer to 9.7.6 - Creating a priority policy on page 216.
4	Apply the priority policy on the desired interface. Refer to 9.7.7 - Applying a priority policy on an interface on page 218.

9.7.4 Creating a traffic policy on the router

Refer to 9.7.3 - How to configure a traffic and priority policy on the router? on page 212 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- → **Create and configure a routing traffic policy. ← You are here.**
- Apply the routing traffic policy on the desired interface.
- Create and configure a priority policy.
- Apply the priority policy on the desired interface.

To create and configure a traffic policy for the routed data on a certain interface, proceed as follows:

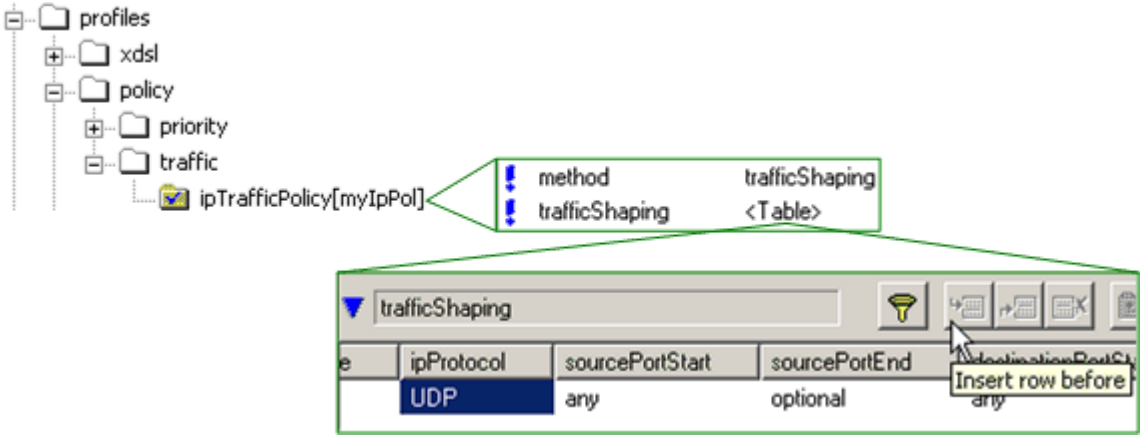
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>In the Telindus 2400 containment tree, go to the profiles/policy/traffic object and add a ipTrafficPolicy[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56).
E.g. ipTrafficPolicy[myIpPol]
</td></tr>
<tr><td>2</td><td>In the ipTrafficPolicy[ ] object you just added, go to the method attribute. Use this attribute to choose a traffic policy method. This traffic policy is then used to determine, on traffic overload conditions, how and which queues are filled with the “excess” data.
 

Refer to telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method on page 381 for more information.</td></tr>
<tr><td>3</td><td>Now, depending on which traffic policy method you selected, you have to configure the actual policy criteria:
<table>
<tr><th>If you choose the method …</th><th>then use the following attribute to configure the policy criteria:</th></tr>
<tr><td>trafficShaping,</td><td>• trafficShaping.
• dropLevels (only the dropLevel1 element).</td></tr>
<tr><td>tosDiffServ,</td><td>dropLevels.</td></tr>
<tr><td>tosMapped,</td><td>• tos2QueueMapping.
• dropLevels (only the dropLevel1 element).</td></tr>
</table>
For more information, refer to …
• telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping on page 382.
• telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/dropLevels on page 385.
• telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping on page 387.</td></tr>
</table>

Example - creating a traffic policy on the router

Suppose you create a traffic policy which uses the traffic shaping method to fill the queues, on traffic overload conditions, with the “excess” data. Suppose you want to do this for the UDP protocol only.

The following figure shows how to configure this:



9.7.5 Applying a traffic policy on an interface of the router

Refer to 9.7.3 - How to configure a traffic and priority policy on the router? on page 212 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create and configure a routing traffic policy.
- → **Apply the routing traffic policy on the desired interface.** ← **You are here.**
- Create and configure a priority policy.
- Apply the priority policy on the desired interface.

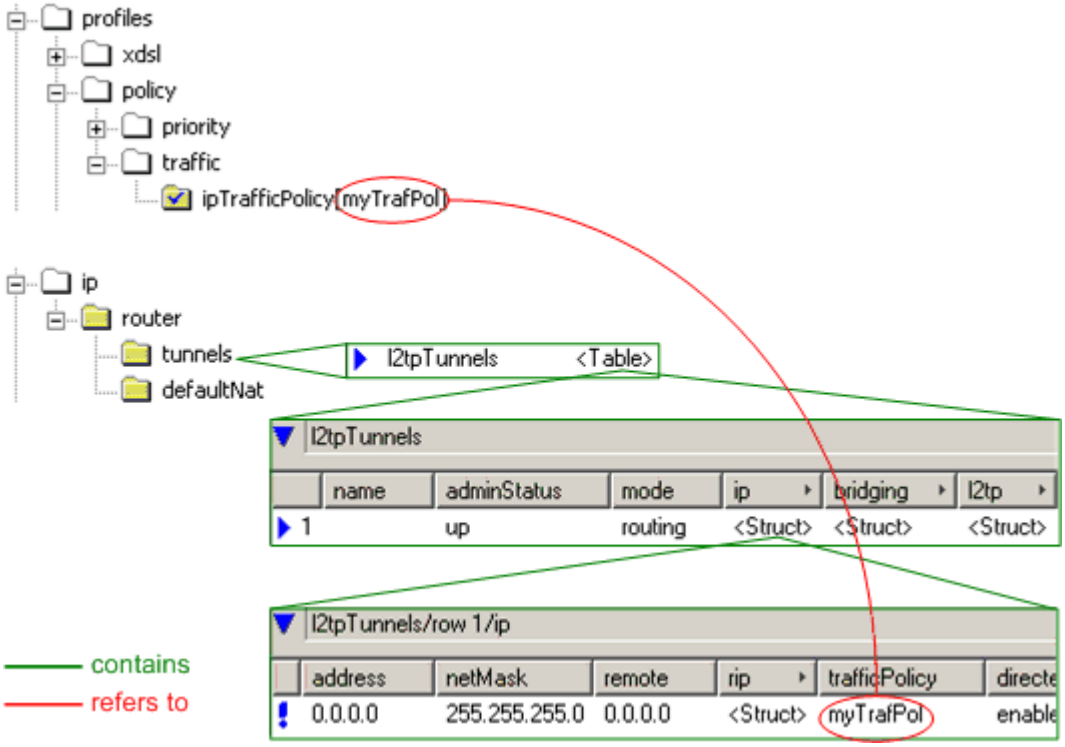
To apply a traffic policy for the routed data on a certain interface, enter the index name of the earlier created ipTrafficPolicy[ ] object as value of the trafficPolicy element. The trafficPolicy element can be found in the ip structure of the IP interface. Refer to 6.2.2 - Where to find the IP parameters? on page 89 for the location of the ip structure on the different IP interfaces.

On the LAN interface, you can not apply a traffic policy with the purpose of queuing. On this interface, the traffic policy is intended to serve as extended access list. Refer to 12.2 - Configuring an extended access list on page 271.

Example - applying a traffic policy on an interface of the router

Suppose you created and configured a traffic policy object with index name myTrafPol (i.e. ipTrafficPolicy[myTrafPol]), and you want to apply this traffic policy on an L2TP tunnel you created earlier.

The following figure shows how to configure this:



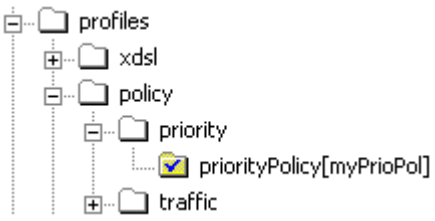
9.7.6 Creating a priority policy

Whereas configuring a traffic policy for routed data is different than for bridged data, configuring a priority policy is the same for both. In other words, the mechanism to fill the queues is different for routed data than it is for bridged data, but the mechanism to empty the queues is the same for both routed and bridged data.

Refer to 9.7.3 - How to configure a traffic and priority policy on the router? on page 212 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create and configure a traffic policy.
- Apply the traffic policy on the desired interface.
- → **Create and configure a priority policy.** ← **You are here.**
- Apply the priority policy on the desired interface.

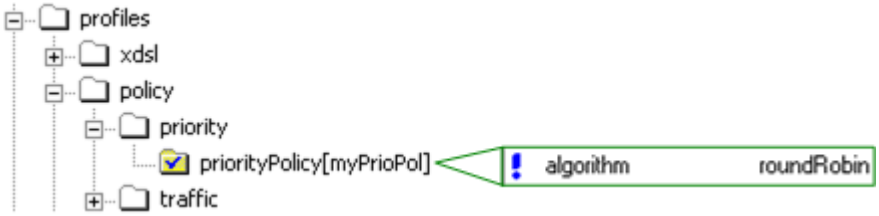
To create and configure a priority policy for a certain interface, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the profiles/policy/priority object and add a priorityPolicy[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56). E.g. priorityPolicy[myPrioPol] 
2	In the priorityPolicy[ ] object you just added, go to the algorithm attribute. Use this attribute to determine how and which queues are emptied. Refer to telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm on page 391 for more information.
3	Configure the other attributes in the priorityPolicy[ ] object. The most important are: • queueConfigurations. Use this attribute to … - set the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed. - set the relative importance of the user configurable queues. Refer to telindus24xx/profiles/policy/priority/priorityPolicy[ ]/queueConfigurations on page 394 for more information. • lowDelayQuotum. Use this attribute to set the number of bytes/packets that is dequeued from the low delay queue when the queue is addressed. Refer to telindus24xx/profiles/policy/priority/priorityPolicy[ ]/lowdelayQuotum on page 394 for more information.

Example - creating a traffic policy on the router

Suppose you create a priority policy which uses the round-robin algorithm to empty the queues.

The following figure shows how to configure this:



9.7.7 Applying a priority policy on an interface

Refer to 9.7.3 - How to configure a traffic and priority policy on the router? on page 212 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create and configure a traffic policy.
- Apply the traffic policy on the desired interface.
- Create and configure a priority policy.
- → **Apply the priority policy on the desired interface.** ← **You are here.**

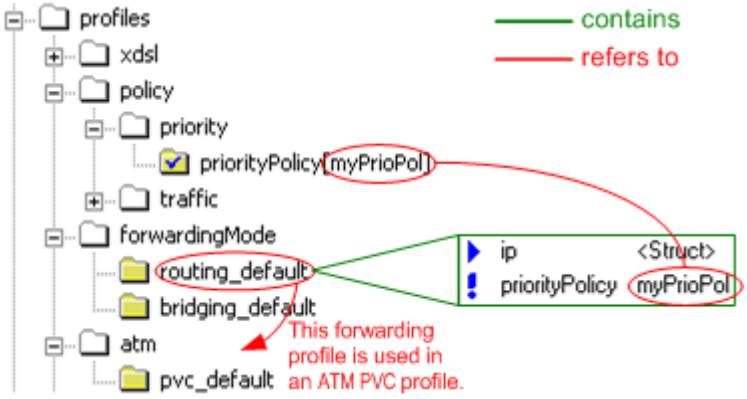
To apply a priority policy on a certain interface, enter the index name of the earlier created priorityPolicy[ ] object as value of the priorityPolicy attribute. The priorityPolicy attribute can be found in …

- profiles/forwardingMode/routing. Use the priorityPolicy attribute in this object in case you applied a IP traffic policy on the routed data of (a) certain interface(s) (profiles/policy/traffic/ipTrafficPolicy[ ]). The routing forwarding profile is then used in an ATM PVC profile which, eventually, is applied on an xDSL interface. So the priority policy is actually applied on an ATM PVC which is present on an xDSL interface.
- profiles/forwardingMode/bridging. Use the priorityPolicy attribute in this object in case you applied a bridging traffic policy on the bridged data of (a) certain interface(s) (profiles/policy/traffic/bridgingTrafficPolicy[ ]). The bridging forwarding profile is then used in an ATM PVC profile which, eventually, is applied on an xDSL interface. So the priority policy is actually applied on an ATM PVC which is present on an xDSL interface.
- bundle/imaGroup[ ]/pvc. Use the priorityPolicy element in the pvc table in case you applied an IP or bridging traffic policy on (a) certain interface(s) (profiles/policy/traffic/ipTrafficPolicy[ ] or bridgingTrafficPolicy[ ]). So the priority policy is applied on an ATM PVC which is part of an IMA group which, on its turn, is present on the 6E1 interface.

Example - applying a priority policy on an interface

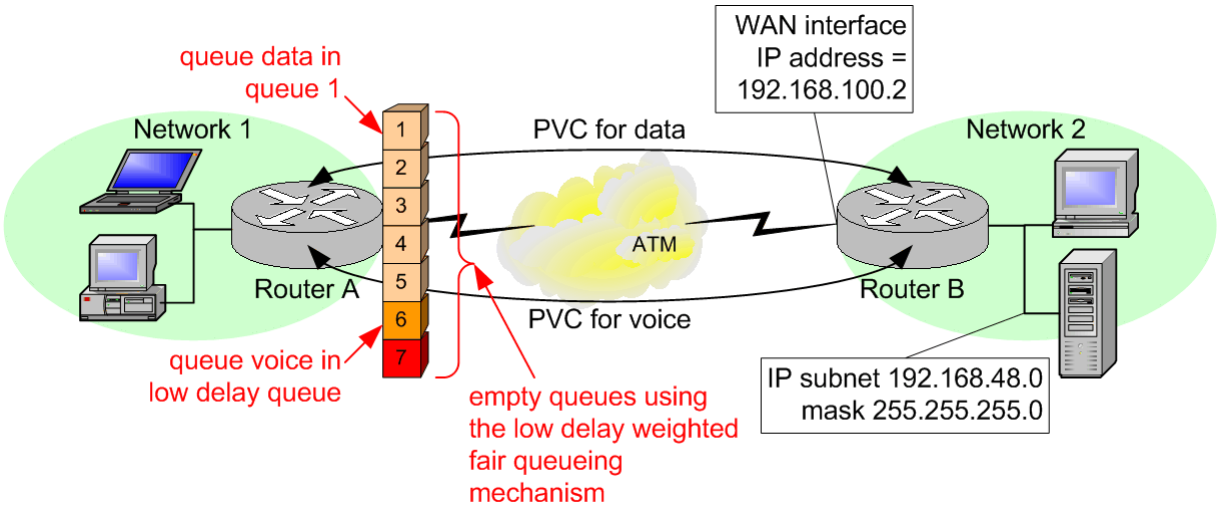
Suppose you created and configured a priority policy object with index name myPrioPol (i.e. priorityPolicy[myPrioPol]), and you want to apply this priority policy on an ATM PVC profile you created earlier.

The following figure shows how to configure this:



9.7.8 Configuring a traffic and priority policy on the router - an example

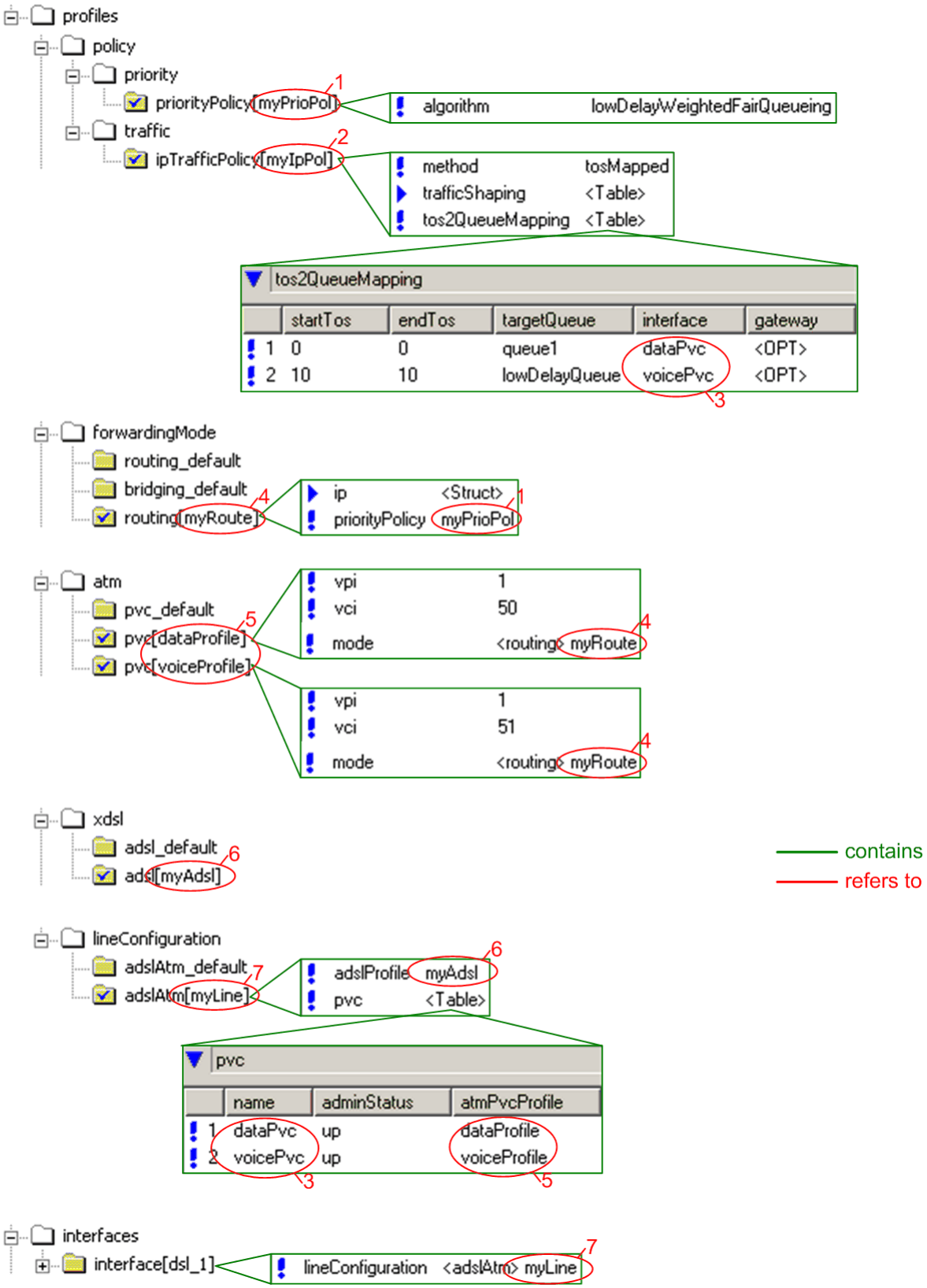
Suppose you have two networks which are interconnected via an xDSL link over an ATM network. Network 1 carries a mix of data and voice traffic. The traffic on this network is differentiated by setting the Type Of Service (TOS) values in the IP packet headers (data = 0, voice = 10). When the traffic is routed from network 1 to network 2 you want that the data traffic and the voice traffic each go over a separate PVC on xDSL line 1. What is more, if congestion should occur you want that the voice is queued in the low delay queue and that the data is queued in queue 1. The algorithm that you want to use to empty the queues is the low delay weighted fair queueing mechanism.

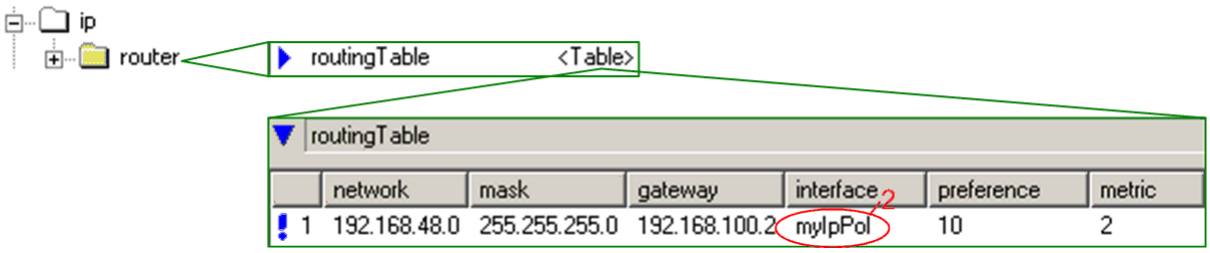


Sketched in broad outlines, this is how you configure the above:

Step	Action
1	Create and apply the necessary profiles to configure the xDSL line and to set up the ATM PVCs. For example: • Define one ATM PVC that will carry the data traffic, e.g. pvc/name = dataPvc. • Define another ATM PVC that will carry the voice traffic, e.g. pvc/name = voicePvc. • Activate these ATM PVCs on xDSL line 1. Since this is not the main subject of this example, refer for more information on creating ATM PVCs on xDSL lines to 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126.
2	Create and configure an IP traffic policy for policy based routing and queueing purposes. For example: • Create an ipTrafficPolicy[myIpPol] object. • Set the method attribute to tosMapped. • In the tos2QueueMapping structure, create two entries and define the startTos, endTos and interface elements of each entry in such a way that the data traffic and the voice traffic each go over a separate PVC. Also set the targetQueue for both types of traffic: - the low delay queue for the voice. - queue 1 for the data.
3	Create a route that “points” to this traffic policy. For example: Create an entry in the routingTable attribute in which you specify that traffic destined for network 192.168.48.0 has to be sent to the IP traffic policy you created earlier.

The following figure shows how to configure the traffic and priority policy you want to set up:




ip
router
routingTable
<Table>
routingTable
network
mask
gateway
interface
preference
metric
1
192.168.48.0
255.255.255.0
192.168.100.2
myIpPol
10
2

10 Configuring bridging

This chapter introduces bridging on the Telindus 2400 and lists the attributes you can use to configure bridging.

The following gives an overview of this chapter:

- 10.1 - Introducing bridging on page 224
- 10.2 - Configuring bridging on page 234
- 10.3 - Configuring traffic and priority policy on the bridge on page 245

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

10.1 Introducing bridging

This section introduces the bridging concept. The following gives an overview of this section:

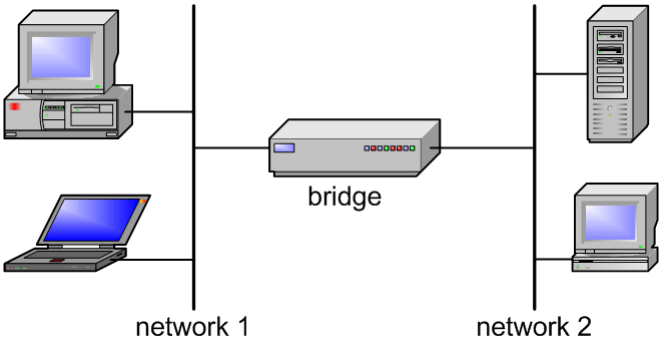
- 10.1.1 - What is bridging? on page 225
- 10.1.2 - The self-learning and Transparent Spanning Tree bridge on page 226
- 10.1.3 - The Spanning Tree root bridge on page 227
- 10.1.4 - The Spanning Tree topology on page 228
- 10.1.5 - The Spanning Tree bridge port states on page 229
- 10.1.6 - The Spanning Tree Bridge Protocol Data Unit on page 230
- 10.1.7 - The Spanning Tree behaviour on page 231
- 10.1.8 - The Spanning Tree priority and cost on page 232

10.1.1 What is bridging?

The Telindus 2400 can be configured to act as a bridge. This enables you to split up your LAN network into smaller parts or segments. This decreases the amount of data traffic on the separated LAN segments and, consequently, increases the amount of available bandwidth.

Example

The following figure shows an example of bridging:



Data coming from network 1, will only be let through by the bridge if this data has a destination outside network 1 or if it has a broadcast or multicast address. This means the bridge filters the data and decreases the amount of data traffic on the separated LAN segments.

10.1.2 The self-learning and Transparent Spanning Tree bridge

The Telindus 2400 features two bridging mechanisms:

- self-learning bridging,
- self-learning bridging in conjunction with the Transparent Spanning Tree (TST) algorithm, or briefly Spanning Tree bridging.

Bridging principle	Description
self-learning	The bridge learns which data it has to forward to the other LAN segment and which data it has to block. I.e. it builds its own bridging table. In other words, you do not have to configure a bridging table with MAC addresses of stations that are located on the separated LAN segments but that have to be able to communicate with each other.
self-learning + TST	This is based on the self-learning principle, but a protocol is used to implement the TST algorithm. **Bridging loops** The primary goal of this algorithm is to avoid that bridging loops arise. A bridging loop occurs when two self-learning bridges are placed in parallel. This results in data that keeps circling around as each bridge forwards the same data. **The TST algorithm** Using the TST algorithm, bridges know of each others existence. By communicating with each other, they establish one single path for reaching any particular network segment. If necessary, they may decide to disable some bridges in the network in order to establish this single path. This is a continuous process. So if a bridge fails, the remaining bridges will reconfigure their bridging tables keeping each LAN segment reachable.

10.1.3 The Spanning Tree root bridge

What is the root bridge?

Spanning Tree defines a tree with a root bridge and a loop-free path from the root to all bridges in the extended network. The root bridge is the logical centre of the Spanning Tree topology.

Redundant data paths are forced into a stand-by (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the stand-by path.

How is a root bridge selected?

All bridges in the network participating in Spanning Tree gather information about other bridges in the network. They do this through an exchange of data messages called Bridge Protocol Data Units (BPDUs).

This exchange of messages results in the following phases:

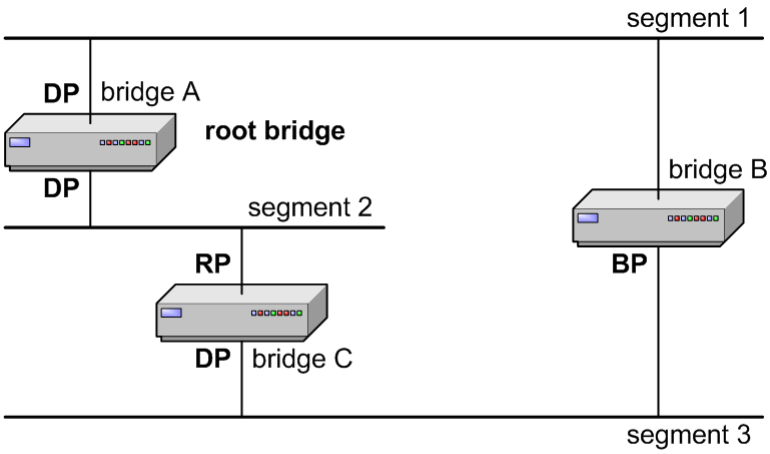
Phase	Description
1	The selection of a root bridge. The bridge with the highest bridge priority (i.e. the lowest numerical priority value) is selected as the root bridge. If all bridges are configured with the default priority (32768), the bridge with the lowest MAC address becomes the root bridge.
2	The selection of a designated bridge for every bridged LAN segment.
3	The removal of loops in the bridged network by blocking bridge ports connected to redundant links.

10.1.4 The Spanning Tree topology

The cost factor is used to calculate the distance from each port of a bridge to the root bridge. On the basis of this, each port on a bridge is assigned one of the following states:

State	Description
root port	The port that is closest to the root bridge. Only one port on each bridge is assigned as the root port.
designated port	The port that connects to bridges further away from the root bridge. The root bridge only has designated ports.
blocking	If a port is not assigned a root port or a designated port state, they are assigned a blocking state. Frames (with the exception of Configuration BPDUs) are not accepted or transmitted by the port when it is in the blocking state. The port can be said to be in stand-by.

An elementary example of a Spanning Tree topology is given in the figure below:



RP = Root Port
DP = Designated Port
BP = Blocking Port

10.1.5 The Spanning Tree bridge port states

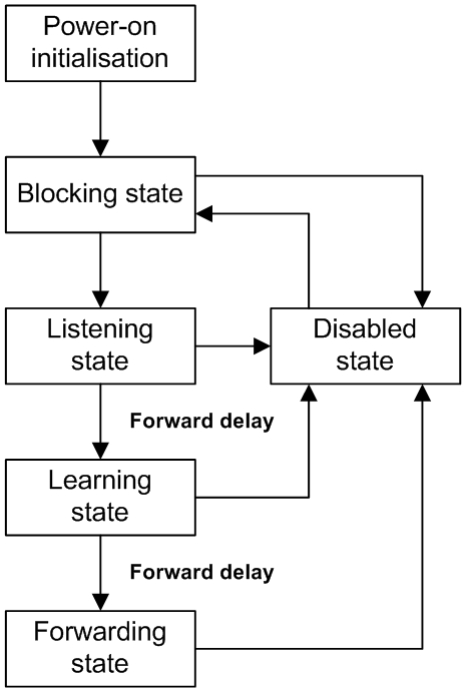
Bridge port states

There are four possible states a bridge port can be in:

State	A port in this state …
blocking	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a blocking port, so there is no MAC address database update.). • receives BPDUs, but does not process or propagate them. A bridge always enters the blocking state following bridge initialisation.
listening	• does no frame forwarding. • does not incorporate station location into its address database (There is no learning on a listening port, so there is no MAC address database update.). • receives and processes BPDUs, but does not propagate them.
learning	• does no frame forwarding. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.
forwarding	• forwards frames. • incorporates station location into its MAC address database. • receives, processes and propagates BPDUs.

Bridge port state transition diagram

The following figure shows how a bridge port moves through the different states when the bridge is powered:



When you enable Spanning Tree, every bridge in the network goes through the transitory states of listening and learning at power up. If properly configured, each port stabilises to the forwarding or blocking state.

When the spanning-tree algorithm places a port in the forwarding state, the following process occurs:

1. The port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
2. The port waits for the expiration of the forward delay timer, moves the port to the learning state, and resets the forward delay timer.
3. In the learning state, the port continues to block frame forwarding as it learns station location information for the forwarding database.
4. The port waits for the expiration of the forward delay timer and then moves the port to the forwarding state, where both learning and forwarding are enabled.

10.1.6 The Spanning Tree Bridge Protocol Data Unit

What is a BPDU?

To establish a stable path, each bridge sends Configuration Bridge Protocol Data Units (BPDUs) to its neighbouring bridges. These Configuration BPDU messages contain information about the spanning tree topology. The contents of these frames only changes when the bridged network topology changes or has not been established.

Each Configuration BPDU contains the following minimal information:

- The unique bridge identifier of the bridge that the transmitting bridge believes to be the root bridge.
- The cost of the path to the root from the transmitting port.
- The unique port identifier of the transmitting port.

When a bridge transmits a BPDU frame, all bridges connected to the LAN on which the frame is transmitted receive the BPDU. When a bridge receives a BPDU, it does not forward the frame. Instead, it uses the information in the frame to:

- calculate a BPDU,
- initiate a BPDU transmission if the topology changes.

The propagation of Configuration BDPUs

When a bridged network is in a stable condition, switches continue to send Configuration BPDUs to its neighbouring bridges at regular intervals. Configuration BPDUs are transmitted down the spanning tree from designated ports to root ports. If a Configuration BPDU is not received by the root port of a bridge within a predefined time interval (for example, because a bridge along the path has dropped out), the port enters the listening state to re-determine a stable path.

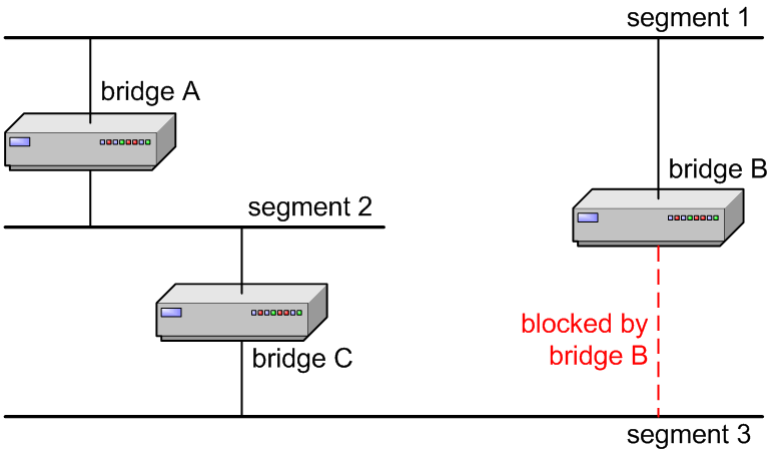
10.1.7 The Spanning Tree behaviour

The following are some examples of how Spanning Tree behaves when certain events occur in your network.

Bridging loops

Bridges connected in a LAN must detect potential bridge loops. They must then remove these loops by blocking the appropriate ports to other bridges.

This is illustrated in the following figure:

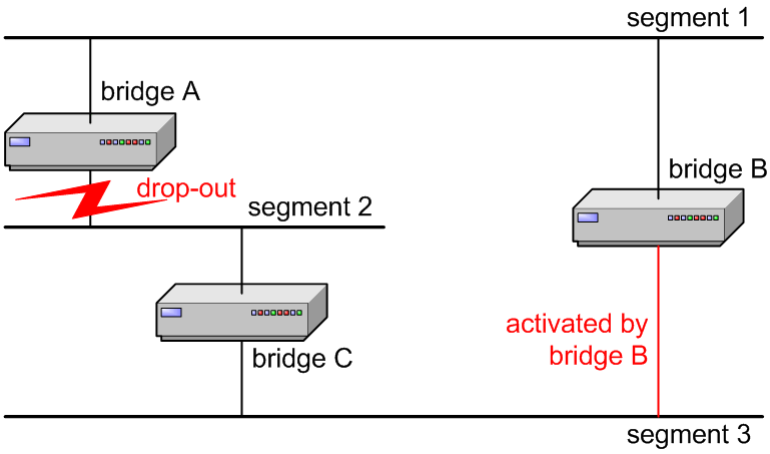


An alternate path has been established by connecting Bridge B in parallel with Bridges A and C. This also creates a potential bridge loop. However, by using the Spanning Tree Algorithm, Bridge B breaks the loop and blocks its path to segment 3.

Bridge failure

Bridges connected in a LAN must also detect bridge failure. They must then establish an alternative path. Should the root bridge fail, also a new root bridge must be selected.

A bridge failure is illustrated in the following figure:

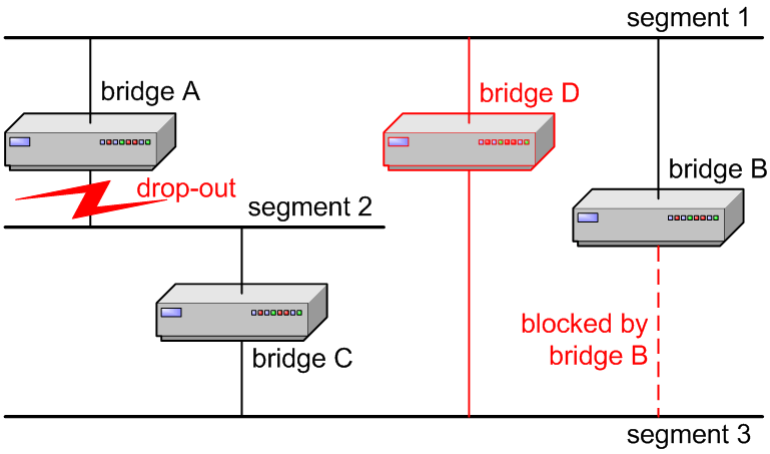


If Bridge A fails, the Spanning Tree Algorithm must be capable of activating an alternative path, such as Bridge B.

Network extension

Bridges connected in a LAN must also detect topology changes. They must adapt to these changes.

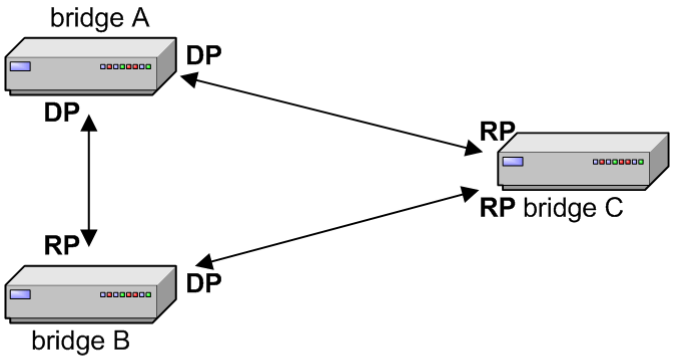
A topology change is illustrated in the following figure:



If the network is extended by adding Bridge D, the Spanning Tree Algorithm must be capable of adapting automatically to the new topology. This means that Bridge B stops looping by blocking the path to segment 3.

10.1.8 The Spanning Tree priority and cost

Consider the following Spanning Tree Topology:



RP = Root Port
DP = Designated Port

What is bridge priority?

In the example above, Bridge A is selected as the root bridge. This because the bridge priority of all the bridges is set to the default value (32768) and Bridge A has the lowest MAC address. However, due to traffic patterns or link types, Bridge A might not be the ideal root bridge.

By increasing the bridge priority (lowering the numerical priority value) of the ideal bridge so that it becomes the root bridge, you force a Spanning Tree recalculation to form a new spanning-tree topology with the ideal bridge as the root.

What is port priority and path cost?

When the spanning-tree topology is calculated based on default parameters, the path between source and destination stations in a bridged network might not be ideal. The goal is to make the fastest link the root port.

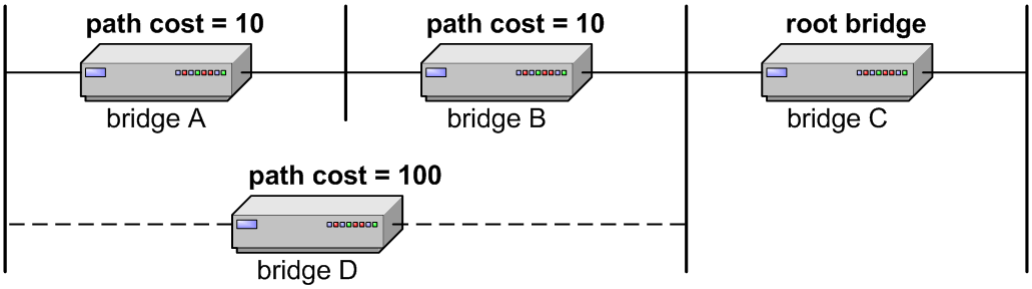
For example, assume on Bridge B that …

- port 1, currently the root port, is an unshielded twisted-pair link,
- port 2 is a fibre-optic link.

Network traffic might be more efficient over the high-speed fibre-optic link. By changing the spanning-tree port priority or path cost for port 2 to a higher priority (lower numerical value) than port 1, port 2 becomes the root port.

Example

By changing the priority and/or the pathCost, you can create a "preferred" path:



By setting the path costs of Bridge A and B to a lower value than the path cost of Bridge D, you can create a *preferred* path through Bridge A and B. The path through Bridge D becomes the *back-up* path.

10.2 Configuring bridging

This section lists the attributes you can use to configure bridging. The following gives an overview of this section:

- 10.2.1 - Introducing the bridging attributes on page 235
- 10.2.2 - Configuring the bridge group on page 236
- 10.2.3 - Adding a bridge group on page 237
- 10.2.4 - Enabling bridging on an interface on page 239
- 10.2.5 - Configuring bridging on an interface on page 240
- 10.2.6 - Explaining the bridging structure on page 241

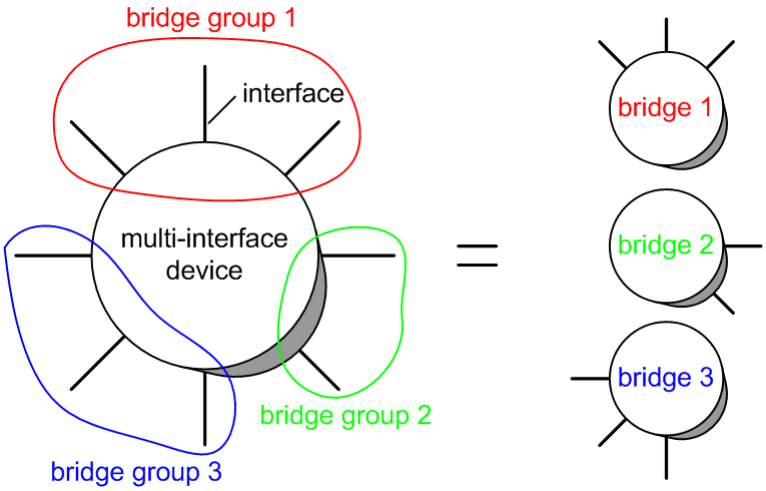
10.2.1 Introducing the bridging attributes

What is a bridge group?

A bridge group comprises the main bridging process. So in the containment tree, the bridgeGroup object contains the general bridging attributes.

What are multiple bridge groups?

The Telindus 2400 offers the possibility to create multiple bridge groups. This means you can group some interfaces in one bridge group while you group several other interfaces in another bridge group. By doing so, it is as if you created several “simple” bridge devices within one device.



Bridging on the different interfaces

In addition to configuring the general bridging process using the configuration attributes of the bridge group, you also have to configure bridging on each interface on which you want to use bridging.

10.2.2 Configuring the bridge group

Refer to …

- 10.1 - Introducing bridging on page 224 for an introduction on bridging.
- 10.2.1 - Introducing the bridging attributes on page 235 for an introduction on the bridging attributes.

This section lists the most important configuration attributes of the bridge group.

Configuring an IP address on the bridge group

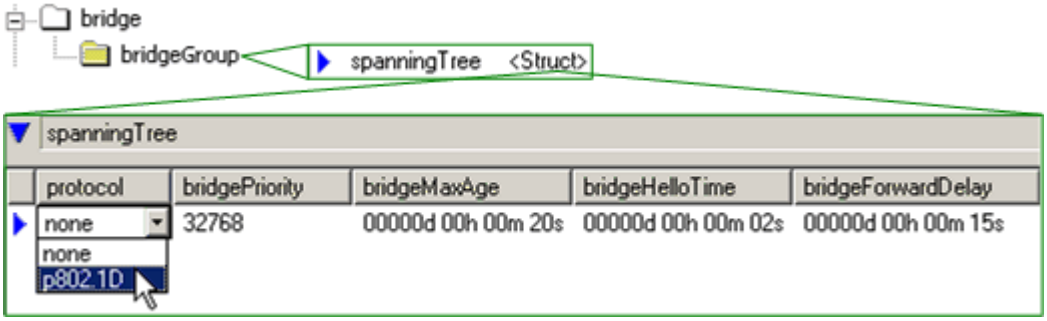
As on other interfaces (LAN, PVCs, etc.), you can configure an IP address on the bridge group. Do this using the configuration attribute telindus24xx/bridge/bridgeGroup/ip on page 447.

What is more, if you enable bridging on the LAN interface (telindus24xx/lanInterface/mode = bridging), then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. So in this case, if you want to manage the Telindus 2400 via IP, then you have to configure an IP address in the bridgeGroup object instead.

Selecting the bridging protocol

Refer to 10.1.2 - The self-learning and Transparent Spanning Tree bridge on page 226 for an introduction.

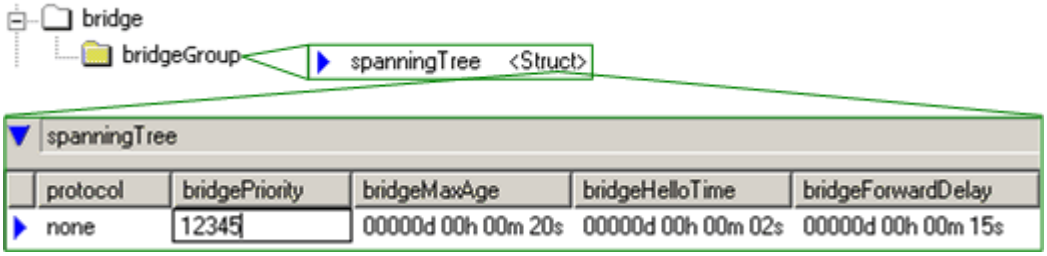
Use the protocol element in the spanningTree structure to select the bridging protocol. Refer to telindus24xx/bridge/bridgeGroup/spanningTree on page 449.



Setting the bridge priority

Refer to 10.1.8 - The Spanning Tree priority and cost on page 232 for more information on bridge priority.

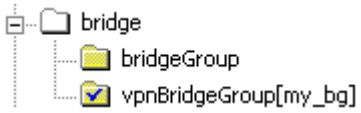
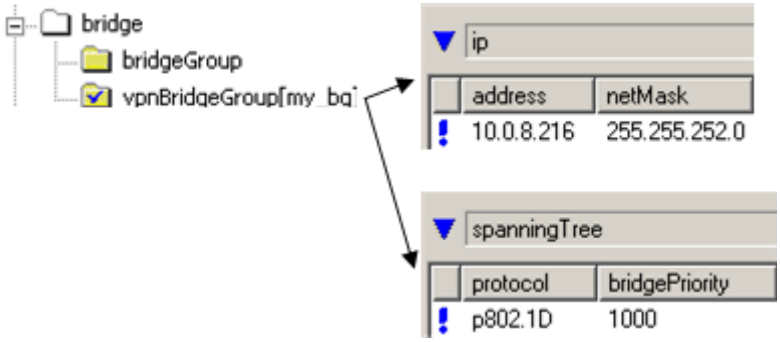
Use the bridgePriority element in the spanningTree structure to set the bridge priority. Refer to telindus24xx/bridge/bridgeGroup/spanningTree on page 449.



10.2.3 Adding a bridge group

As said in 10.2.1 - Introducing the bridging attributes on page 235, you can add several bridge groups.

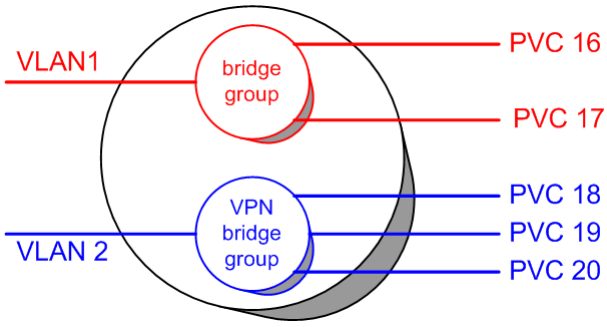
In order to add a bridge group, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the bridge object and add a vpnBridgeGroup[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56).  E.g. vpnBridgeGroup[my_bg]
2	In the vpnBridgeGroup[ ] object you just added, configure the attributes to your needs. Example: Suppose you configure an IP address on the bridge group, activate the spanning tree protocol and set a bridge priority. 
3	Now you can add interfaces to the bridge group you just created. Do this by entering the name of the bridge group in the bridging/bridgeGroup element of the interfaces you want to add. Refer to 10.2.6 - Explaining the bridging structure on page 241 (more specifically to the bridgeGroup element) for more information. Example: Suppose you want to add the LAN interface to the vpnBridgeGroup[my_bg] object you previously added, then type the string “my_bg” in the bridgeGroup element of the bridging structure of the lanInterface object.

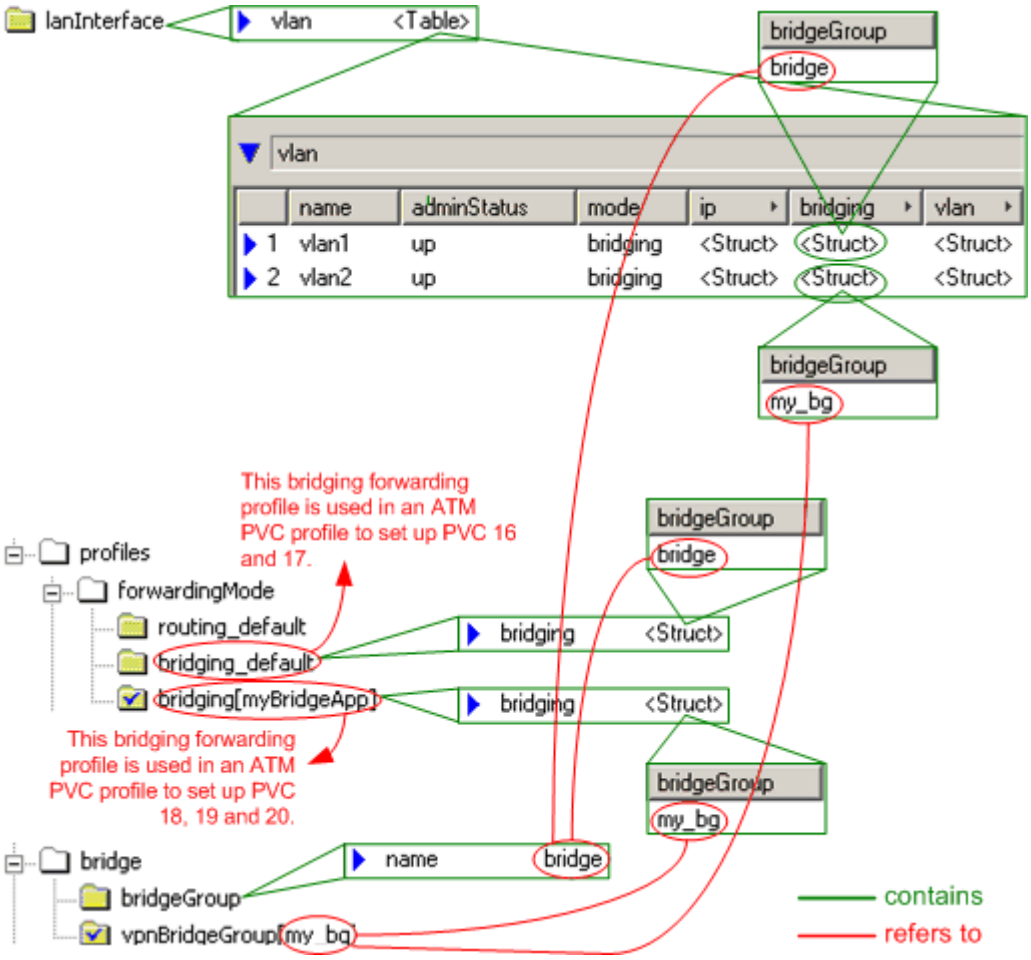
Example - multiple bridge groups

Suppose …

- you have 2 VLANs (VLAN 1 and VLAN 2).
- you have 5 DLCIs (DLCI 16 up to DLCI 20).
- you want to assign VLAN 1 and DLCI 16 and 17 to the default bridge group.
- you want to assign VLAN 2 and DLCI 18, 19 and 20 to a bridge group you added yourself.



So first, add a bridge group to the containment tree (e.g. vpnBridgeGroup[my_bg]. Then assign the different interfaces to the different bridge groups by specifying bridge group names in the bridging/bridgeGroup elements of the different interfaces. Also set the different interfaces in bridging mode.



10.2.4 Enabling bridging on an interface

Refer to …

- 10.1 - Introducing bridging on page 224 for an introduction on bridging.
- 10.2.1 - Introducing the bridging attributes on page 235 for an introduction on the bridging attributes.

Per IP interface you can determine whether you perform routing, bridging or both. The following table shows, for each IP interface, how to enable bridging on this interface:

Interface	How to enable bridging?
LAN interface	Set the mode attribute to bridging or routingAndBridging. The mode attribute can be found in the lanInterface object: telindus24xx/lanInterface/mode. **Important remark** If you set the configuration attribute telindus24xx/lanInterface/mode to bridging (default setting!), then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. So in this particular case, if you want to manage the Telindus 2400 via IP, then you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.
4 port Ethernet interface	Set the mode attribute to bridging or routingAndBridging. The mode attribute can be found in the 4pEth object: telindus24xx/4pEth/mode.
VLAN on the LAN interface	Set the mode element to bridging. The mode element can be found in the vlan table which is located in the lanInterface object: telindus24xx/lanInterface/vlan/mode.
VLAN on the 4 port Ethernet interface	Set the mode element to bridging. The mode element can be found in the vlan table which is located in the 4pEth object: telindus24xx/4pEth/vlan/mode.
ATM PVC on the xDSL lines	Set the mode attribute to bridging, then determine which bridging forwarding profile has to be applied on the ATM PVC profile. The mode attribute can be found in the profiles/atm/pvc_default or profiles/atm/pvc[ ] object: telindus24xx/profiles/atm/pvc_default/mode. Refer to 5.2.2 - How to apply the forwarding profile? on page 77.
ATM PVC on the 6E1 interface	Set the mode element to bridging. The mode element can be found in the pvc table which is located in the imaGroup object: telindus24xx/bundle/imaGroup[ ]/pvc/mode.
ATM PVC on the E3/T3 interface	Set the mode element to bridging. The mode element can be found in the pvc table which is located in the e3T3[E3T3_x]/atm object: telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/mode.
L2TP tunnel	Set the mode element to bridging or routingAndBridging. The mode element can be found in the l2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/l2tpTunnels/mode.
IPSEC L2TP tunnel	Set the mode element to bridging or routingAndBridging. The mode element can be found in the ipsecL2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/mode.

10.2.5 Configuring bridging on an interface

Refer to …

- 10.1 - Introducing bridging on page 224 for an introduction on bridging.
- 10.2.1 - Introducing the bridging attributes on page 235 for an introduction on the bridging attributes.

Once the bridging process is enabled on the interface (refer to 10.2.4 - Enabling bridging on an interface on page 239) you can configure the bridging parameters of this interface. Use the elements in the bridging structure for this purpose. The following table shows you the location of the bridging structure for each interface:

Interface	Location of the bridging parameters
LAN interface	In the bridging structure of the lanInterface object: telindus24xx/lanInterface/bridging.
4 ports Ethernet interface	In the bridging structure of the 4pEth object: telindus24xx/4pEth/bridging.
VLAN on the LAN interface	In the bridging structure of the vlan table which is located in the lanInterface object: telindus24xx/lanInterface/vlan/bridging.
VLAN on the 4 ports Ethernet interface	In the bridging structure of the vlan table which is located in the 4pEth object: telindus24xx/4pEth/vlan/bridging.
ATM PVC on the xDSL lines	In the bridging structure of the bridging forwarding profile: telindus24xx/profiles/forwarding-Mode/bridging_default/bridging. By applying this profile on the ATM PVC profile, the bridging parameters of the ATM PVC are configured.
ATM PVC on the 6E1 interface	In the bridging structure of the pvc table which is located in the imaGroup[ ] object: telindus24xx/bundle/imaGroup[ ]/pvc/bridging.
ATM PVC on the E3/T3 interface	In the bridging structure of the pvc table which is located in the e3T3[E3T3_x]/atm object: telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/bridging.
L2TP tunnel	In the bridging structure of the l2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/l2tpTunnels/bridging.
IPSEC L2TP tunnel	In the ip structure of the ipsecL2tpTunnels table which is located in the tunnels object: telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/bridging.

Refer to 10.2.6 - Explaining the bridging structure on page 241 for a detailed explanation of the bridging structure.

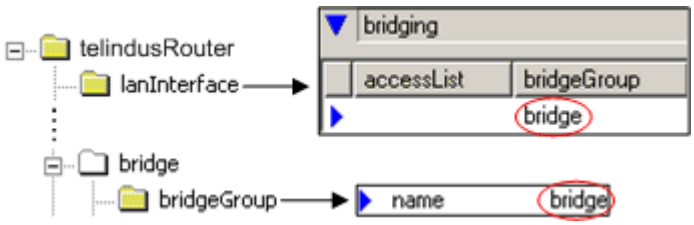
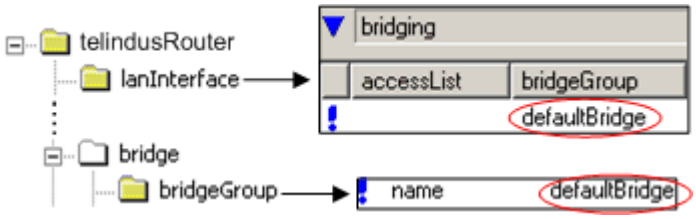
10.2.6 Explaining the bridging structure

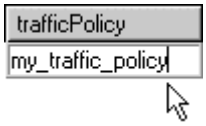
Because the bridging structure occurs in several objects, it is described here once and referenced where necessary. Refer to 10.2.5 - Configuring bridging on an interface on page 240 for the location of the bridging structure.

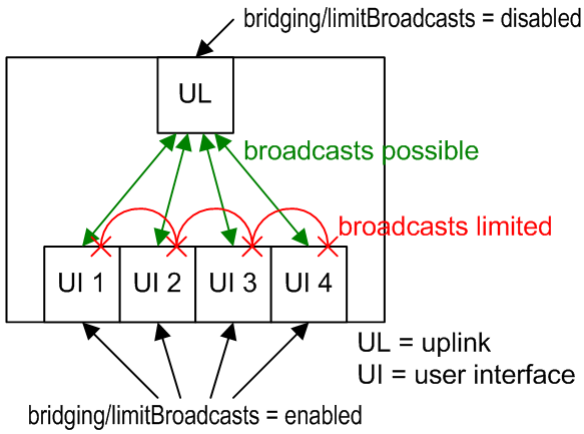
This section lists all the elements that can be present in the bridging structure. However, depending on the interface, it is possible that not all of these elements are present.

The bridging structure contains the following elements:

Element	Description
accessList	Use this element set up an access list on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the access list you want to use. You can create the access list itself by adding an accessList object under the bridge object and by configuring the attributes in this object. **Example** If you created a accessList object with index name my_access_list (i.e. accessList[my_access_list]) and you want to apply this access list here, then enter the index name as value for the accessList element. Refer to … • 13.13.2 - Bridge access list configuration attributes on page 454 for more information on access lists. • 4.4 - Adding an object to the containment tree on page 56 for more information on adding objects.

Element	Description
bridgeGroup	Use this element to determine to which bridge group the interface belongs. Default:bridge Range: 1 … 24 characters You have the possibility to create multiple bridge groups (refer to 10.2.3 - Adding a bridge group on page 237). Then, you can assign some interfaces to one bridge group while you assign several other interfaces to another bridge group. By default, the interface is assigned to the default bridge group (provided the configuration attribute telindus24xx/bridge/bridgeGroup/name of the default bridge group still has its default value "bridge"). You can assign the interface to another bridge group than the default bridge group by specifying the index name of the bridge group in the bridgeGroup element. **Examples** • By default, both the bridgeGroup element and the configuration attribute telindus24xx/bridge/bridgeGroup/name of the default bridge group are set to "bridge". This means that by default the interface is assigned to the default bridge group.  • Suppose you change the name of the default bridge group (by changing the value of the configuration attribute telindus24xx/bridge/bridgeGroup/name). If you still want to assign the interface to the default bridge group, then you have to enter the new name of the default bridge group in the bridgeGroup element of the interface.  • Suppose you add a bridge group with index name my_bg and you want to assign the interface to this bridge group, then enter the index name as value for the bridgeGroup element.

Element	Description
trafficPolicy	This element is not present in the telindus24xx/lanInterface/bridging structure. Use this element to apply a traffic policy on the bridged data on the interface. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the traffic policy you want to use. You can create the traffic policy itself by adding a bridgingTrafficPolicy object under the profiles/policy/traffic object and by configuring the attributes in this object. **Example** If you created a bridgingTrafficPolicy object with index name my_traffic_policy (i.e. bridgingTrafficPolicy[my_traffic_policy]) and you want to apply this traffic policy here, then enter the index name as value for the trafficPolicy element.  Refer to … • 10.3 - Configuring traffic and priority policy on the bridge on page 245 for more information on policies. • 4.4 - Adding an object to the containment tree on page 56 for more information on adding objects.
priority	Use this element to set the port priority of the interface. Default:128 Range: 0 … 255 Each port of a bridge has a *unique port identifier*. The priority element is a part of this port identifier and allows you to change the priority of the port. It is taken as the more significant part in priority comparisons. The other part of the unique port identifier has a fixed relationship to the physical or logical port. This assures the uniqueness of the unique port identifier among the ports of a single bridge. Refer to 10.1.8 - The Spanning Tree priority and cost on page 232 for more information on port priority.
pathCost	Use this element to set the path cost of the interface. Default:100 Range: 1 … 65535 The path cost is the value that is added to the total cost of the path to the root bridge, provided that this particular port is a root port. I.e. that the path to the root goes through this port. The total cost of the path to the root bridge should not exceed 65500. Refer to 10.1.8 - The Spanning Tree priority and cost on page 232 for more information on port priority.
topologyChange-Detection	Use this element to enable or disable the communication of Spanning Tree topology changes to the root bridge. Default:enabled Range: enabled / disabled

Element	Description
limitBroadcasts	Use this element to limit broadcasts between interfaces for which the limitBroadcasts element is set to enabled. Default:disabled Range: enabled / disabled **Example** Suppose you have the following set-up: • Four links towards four different users (clients). • One uplink towards the backbone. • All links are configured for bridging.  In this case you probably want that broadcasts coming from the uplink are distributed to the user links and that broadcasts coming from the user links are forwarded to the uplink. However, you most likely do not want that broadcasts coming from one user link are distributed over all the other user links. Therefore, set the limitBroadcasts element to enabled on all interfaces that may not forward each other's broadcasts.

10.3 Configuring traffic and priority policy on the bridge

Refer to …

- 9.7.1 - Introducing traffic and priority policy on page 208 for an introduction on traffic and priority policy.
- 9.7.2 - Traffic and priority policy on routed and on bridged data on page 211 for the difference between traffic and priority policy on the bridge and the router.

This section gives a short description of the attributes you can use to configure traffic and priority policy on the bridge.

The following gives an overview of this section:

- 10.3.1 - How to configure a traffic and priority policy on the bridge? on page 246
- 10.3.2 - Configuring a traffic policy on the bridge on page 247
- 10.3.3 - Applying a traffic policy on a certain interface of the bridge on page 248

10.3.1 How to configure a traffic and priority policy on the bridge?

Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for an introduction.

To configure a traffic and priority policy for the bridged data on a certain interface, proceed as follows:

Step	Action
1	Create and configure a bridging traffic policy. Refer to 10.3.2 - Configuring a traffic policy on the bridge on page 247.
2	Apply the bridging traffic policy on the desired interface. Refer to 10.3.3 - Applying a traffic policy on a certain interface of the bridge on page 248.
3	Create and configure a priority policy. Refer to 9.7.6 - Creating a priority policy on page 216.
4	Apply the priority policy on the desired interface. Refer to 9.7.7 - Applying a priority policy on an interface on page 218.

10.3.2 Configuring a traffic policy on the bridge

Refer to 10.3.1 - How to configure a traffic and priority policy on the bridge? on page 246 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- → **Create and configure a bridging traffic policy.** ← **You are here.**
- Apply the bridging traffic policy on the desired interface.
- Create and configure a priority policy.
- Apply the priority policy on the desired interface.

To create and configure a traffic policy for the bridged data on a certain interface, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the profiles/policy/traffic object and add a bridgingTrafficPolicy[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56). E.g. bridgingTrafficPolicy[myBridgePol]
2	In the bridgingTrafficPolicy[ ] object you just added, go to the vlanPriorityMap attribute. Use this attribute to impose a traffic policy on the bridged VLAN frames received by the Telindus 2400. Refer to telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/vlanPriorityMap on page 389 for more information.
3	In the bridgingTrafficPolicy[ ] object you just added, go to the dropLevels attribute. Use this attribute to define for each user configurable queue, how many packets may be queued before they are dropped. Refer to telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/dropLevels on page 389 for more information.

10.3.3 Applying a traffic policy on a certain interface of the bridge

Refer to 10.3.1 - How to configure a traffic and priority policy on the bridge? on page 246 for an overview on how to configure a traffic and priority policy. To give you an idea of where you are in the process, the following also gives a quick overview:

- Create and configure a bridging traffic policy.
- → **Apply the bridging traffic policy on the desired interface.** ← **You are here.**
- Create and configure a priority policy.
- Apply the priority policy on the desired interface.

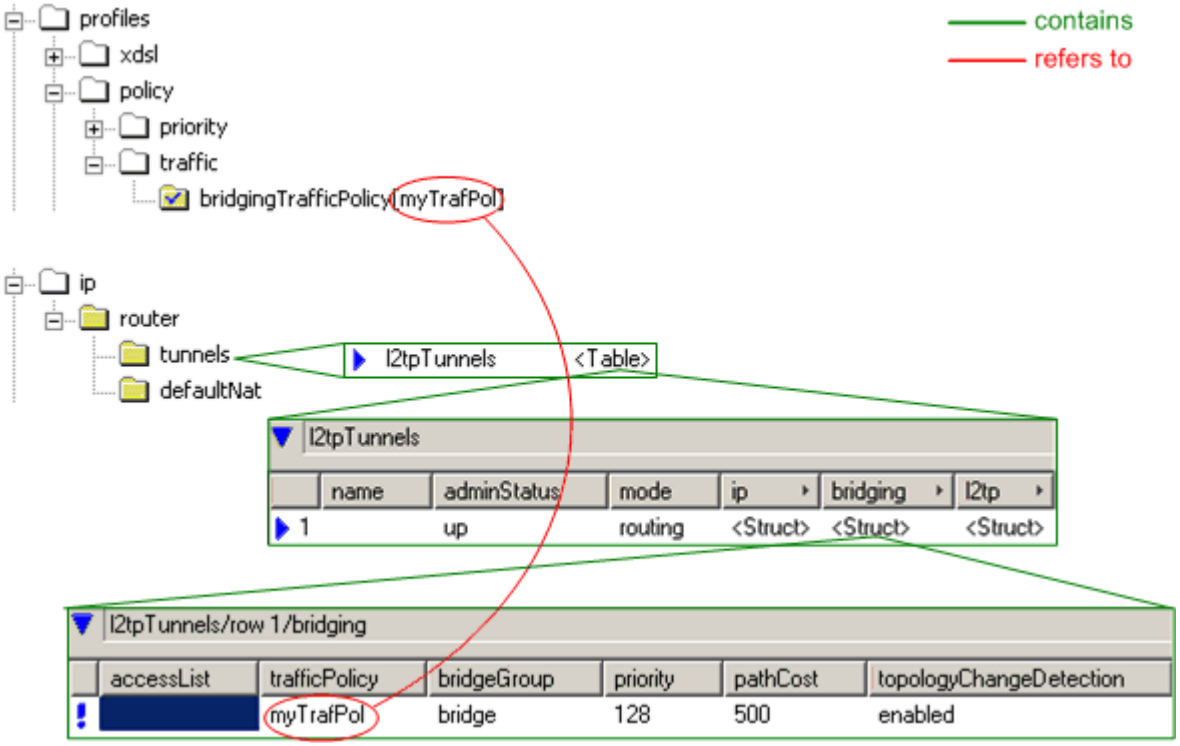
To apply a traffic policy for the bridged data on a certain interface, enter the index name of the earlier created bridgingTrafficPolicy[ ] object as value of the trafficPolicy element. The trafficPolicy element can be found in the bridging structure of the IP interface. Refer to 10.2.5 - Configuring bridging on an interface on page 240 for the location of the bridging structure on the different IP interfaces.

On the LAN interface, you can not apply a bridging traffic policy.

Example - applying a traffic policy on an interface of the bridge

Suppose you created and configured a traffic policy object with index name myTrafPol (i.e. bridgingTrafficPolicy[myTrafPol]), and you want to apply this traffic policy on an L2TP tunnel you created earlier.

The following figure shows how to configure this:



11 Configuring switching

This chapter introduces switching on the Telindus 2400 and lists the attributes you can use to configure switching.

The following gives an overview of this chapter:

- 11.1 - Introducing switching on page 250
- 11.2 - Configuring VLAN switching on page 251
- 11.3 - Configuring ATM switching on page 256

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

11.1 Introducing switching

What is switching?

Switching is somewhat similar to bridging (also see Routing versus bridging on page 166). It also occurs at layer 2 (the link layer) of the OSI reference model. Therefore it is also more of a hardware function and, hence, is faster than routing which occurs at a higher level where the software component is more important.

Which switches are incorporated in the Telindus 2400?

The Telindus 2400 incorporates the following switches:

- a VLAN switch. This switch forwards data from one VLAN to another based on VLAN tags.
- an ATM switch. This switch forwards data from one VP/VC to another based on its VCI/VPI.

The switch contains a table, the switching table, which describes what has to be switched from where to where.

Note the analogy with an Ethernet bridge, which forwards data from one LAN segment to another based on MAC addresses and keeps its information in a bridging table.

11.2 Configuring VLAN switching

This section introduces VLAN switching and gives a short description of the attributes you can use to configure VLAN switching.

The following gives an overview of this section:

- 11.2.1 - Introducing VLAN switching on page 252
- 11.2.2 - How to configure VLAN switching? on page 253

11.2.1 Introducing VLAN switching

Important remark

You can not create VLANs on the LAN interface (refer to 12.3 - Configuring VLANs on page 278) and perform VLAN switching at the same time. So either you create VLANs on the LAN interface or you perform VLAN switching.

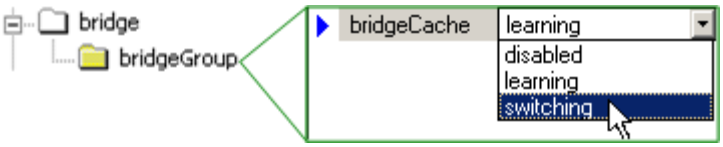
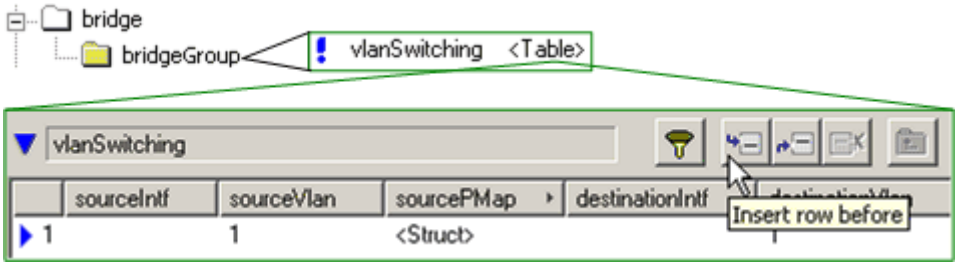
What is VLAN switching?

The basic operation of a VLAN switch is straightforward. A VLAN frame is received on an interface. The switch looks up the VLAN ID value in a local translation table to determine the outgoing interface, the new VLAN ID value of the VLAN frame and, optionally, its new priority. The switch then retransmits the frame on that outgoing interface with the appropriate frame identifiers.

11.2.2 How to configure VLAN switching?

Refer to 11.2.1 - Introducing VLAN switching on page 252 for an introduction.

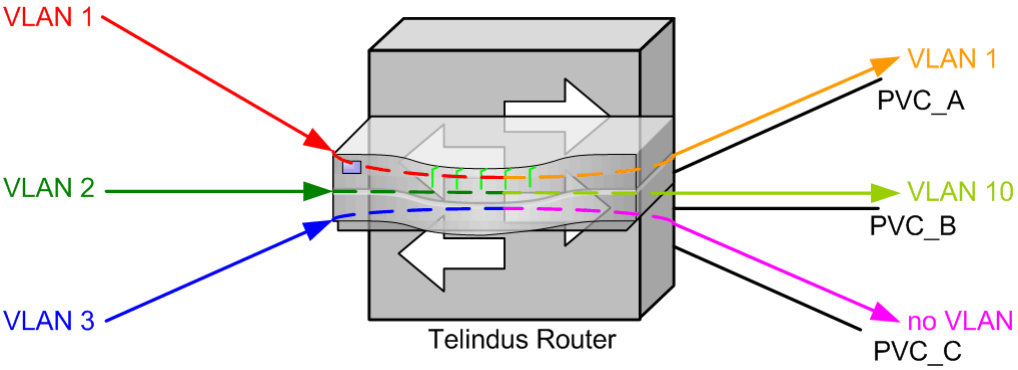
To configure VLAN switching, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the bridge/bridgeGroup object and set the bridgeCache attribute to switching. 
2	In the Telindus 2400 containment tree, go to the bridge/bridgeGroup object, select the vlanSwitching attribute and add one or more entries to this table.  Use this attribute to specify which VLANs you want to switch. Add a row to the vlanSwitching table for each VLAN you want to switch.

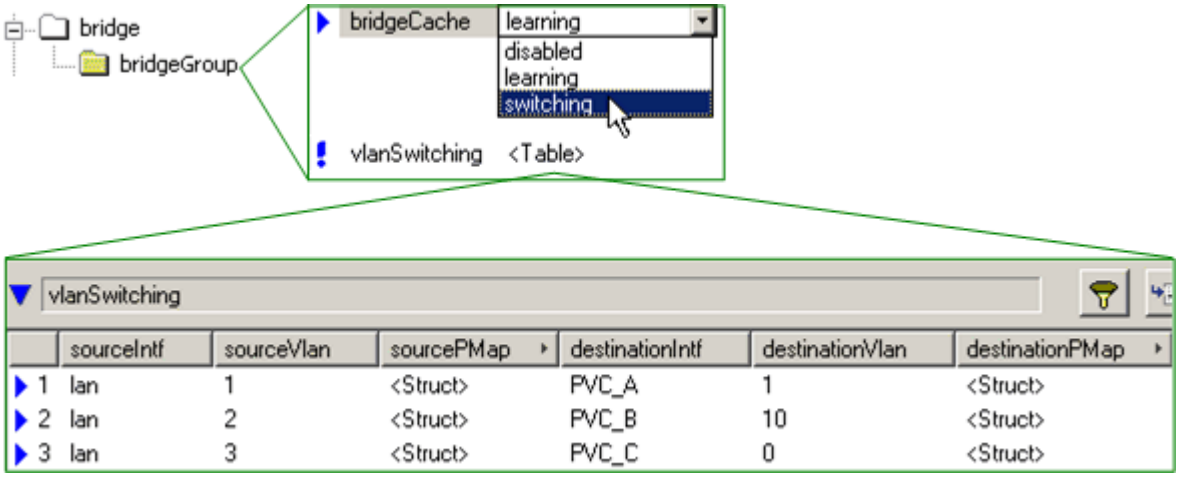
Step	Action
3	Configure the elements of the vlanSwitching table: • sourceIntf. Use this element to enter the name of the (physical) source interface which carries the VLAN that has to be switched. • sourceVlan. Use this element to enter the VLAN ID of the VLAN that has to be switched. Entering 0 as VLAN ID strips the VLAN tag of the Ethernet frame. • sourcePMap. Use this element to, if desired, remap the VLAN priorities. Since the switching is bidirectional, you can remap priorities for both directions (i.e. both at the “source” and “destination” interface). • destinationIntf. Use this element to enter the name of the (physical) destination interface which carries the VLAN when it has been switched. The destination interface can also be a bridge group, in that case just enter the name of the bridge group. • destinationVlan. Use this element to enter the VLAN ID of the VLAN when it has been switched. Entering 0 as VLAN ID strips the VLAN tag of the Ethernet frame. • destinationPMap. Use this element to, if desired, remap the VLAN priorities. Since the switching is bidirectional, you can remap priorities for both directions (i.e. both at the “source” and “destination” interface). **Important remarks** • Note that one row in the vlanSwitching table represents a bidirectional connection. I.e. data is switched from source to destination and vice versa. • Also note that only point-to-point connections are possible. Point-to-multipoint connections are not possible. In other words, a certain VLAN may only appear once in the vlanSwitching table. Refer to telindus24xx/bridge/bridgeGroup/vlanSwitching on page 452 for more information on the elements of the vlanSwitching configuration attribute.

Example - configuring VLAN switching

The following figure shows the LAN interface carrying 3 VLANs that are switched to 3 different ATM PVCs. One of the VLAN IDs is kept, one is changed and one is stripped.



The following figure shows how to configure the bridge group for VLAN switching.



11.3 Configuring ATM switching

This section introduces ATM switching and gives a short description of the attributes you can use to configure ATM switching.

The following gives an overview of this section:

- 11.3.1 - Introducing ATM switching on page 257
- 11.3.2 - How to configure ATM switching? on page 259
- 11.3.3 - How to cascade ATM switches? on page 262

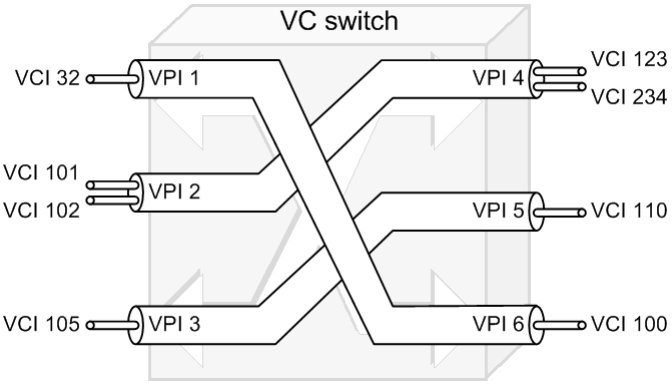
11.3.1 Introducing ATM switching

What is ATM switching?

The basic operation of an ATM switch is straightforward. The cell is received across a link on a known VCI or VPI value. The switch looks up the connection value in a local translation table to determine the outgoing port of the connection and the new VPI/VCI value of the connection on that link. The switch then retransmits the cell on that outgoing link with the appropriate connection identifiers. Because all VCIs and VPIs have only local significance across a particular link, these values are remapped, as necessary, at each switch.

What is VC switching?

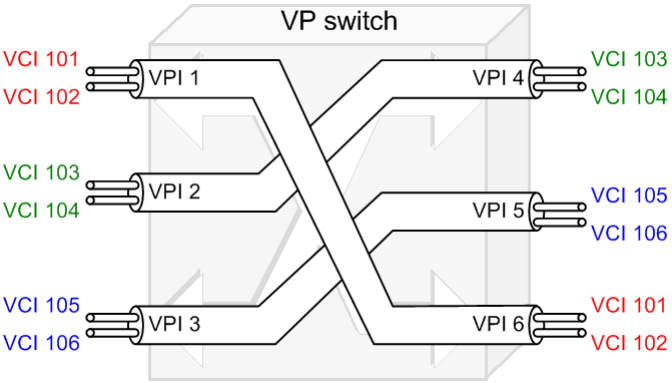
ATM cells arriving on a Virtual Channel (VC) are switched based on both the VPI and VCI number in the cell header. So only one specific VC is switched. This opposed to VP switching where a complete VP (with all its VCs) is switched.



What is VP switching?

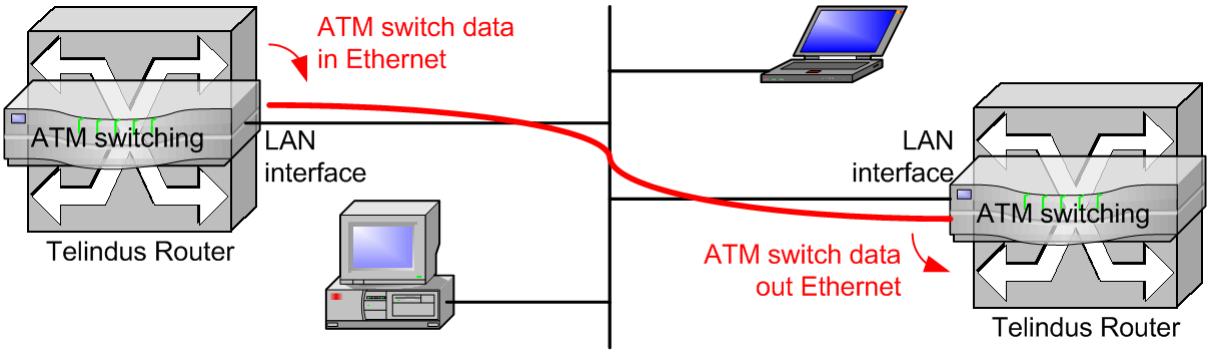
ATM cells arriving on a Virtual Path (VP) are switched based on the VPI number only. So a complete VP (with all its VCs) is switched. This opposed to VC switching where only one specific VC is switched.

Note that in case of VP switching the VCI will remain unchanged for all VCs in the VP. In other words, all VCs in the VP will have same VCI number at the ingress and egress side of the VP (end-to-end).



What is cascading ATM switches?

You can cascade several ATM switches (i.e. several Telindus 2400s configured for ATM switching) over an Ethernet network. This allows you to switch ATM PVCs from one switch to another.

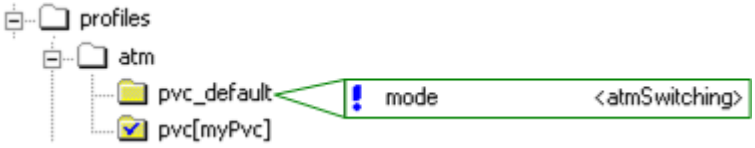
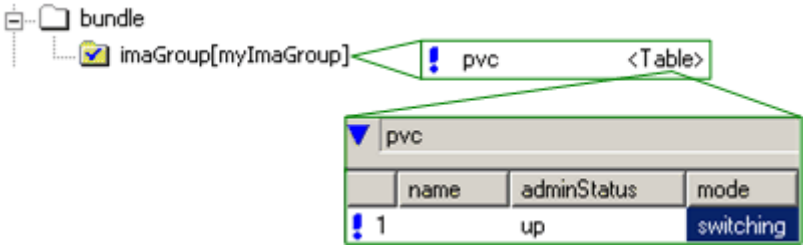
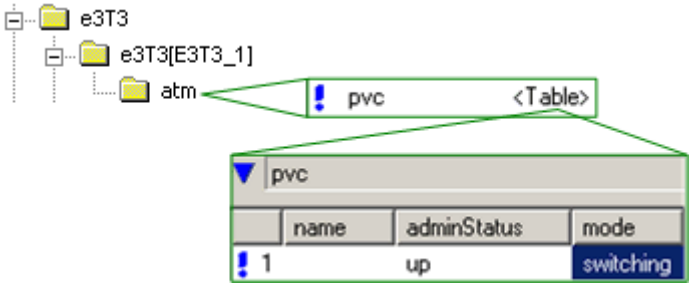
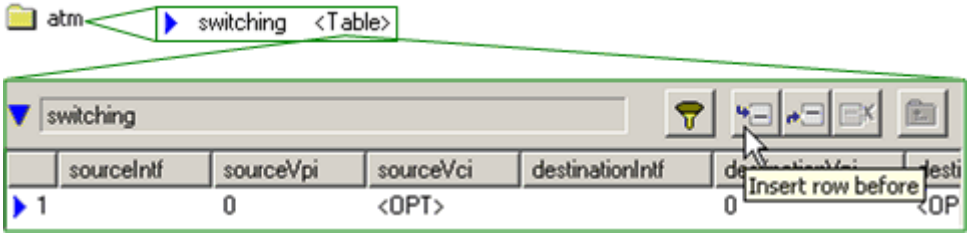


What basically happens is that the raw ATM data coming from one ATM switch is inserted in Ethernet frames, transported over the Ethernet network, extracted out of the Ethernet frames and put in the other ATM switch where it is treated by the switching engine.

11.3.2 How to configure ATM switching?

Refer to 11.3.1 - Introducing ATM switching on page 257 for an introduction.

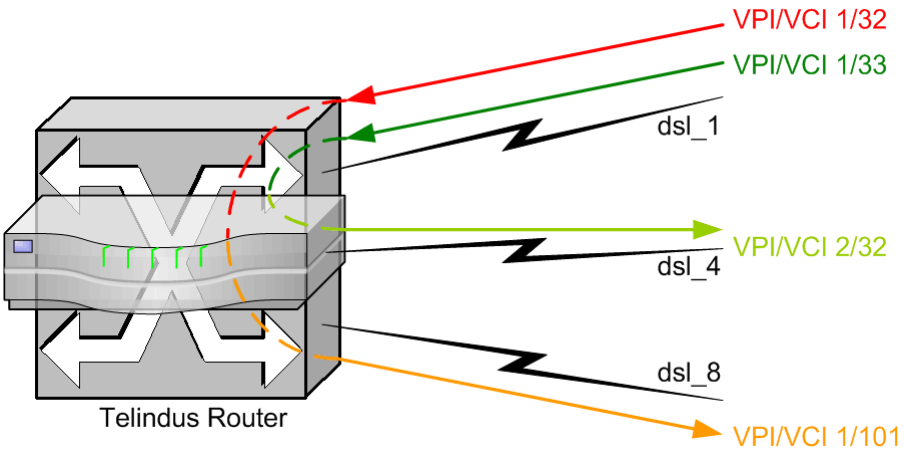
To configure ATM switching, proceed as follows:

Step	Action
1	On the ATM PVCs you want to switch, set the mode to switching. For the ATM PVCs that you can set up on the … • xDSL interfaces, you find the mode attribute in the ATM PVC profile. The profile can be found in: profiles/atm/pvc(_default).  • 6E1 interface (in an IMA group), you find the mode element in the pvc table. The pvc table can be found in: bundle/imaGroup.  • E3/T3 interface, you find the mode element in the pvc table. The pvc table can be found in: e3T3/e3T3[E3T3_x]/atm. 
2	In the Telindus 2400 containment tree, go to the atm object, select the switching attribute and add one or more entries to this table.  Use this attribute to specify which VCs and/or VPs you want to switch. Add a row to the switching table for each VC and/or VP you want to switch.

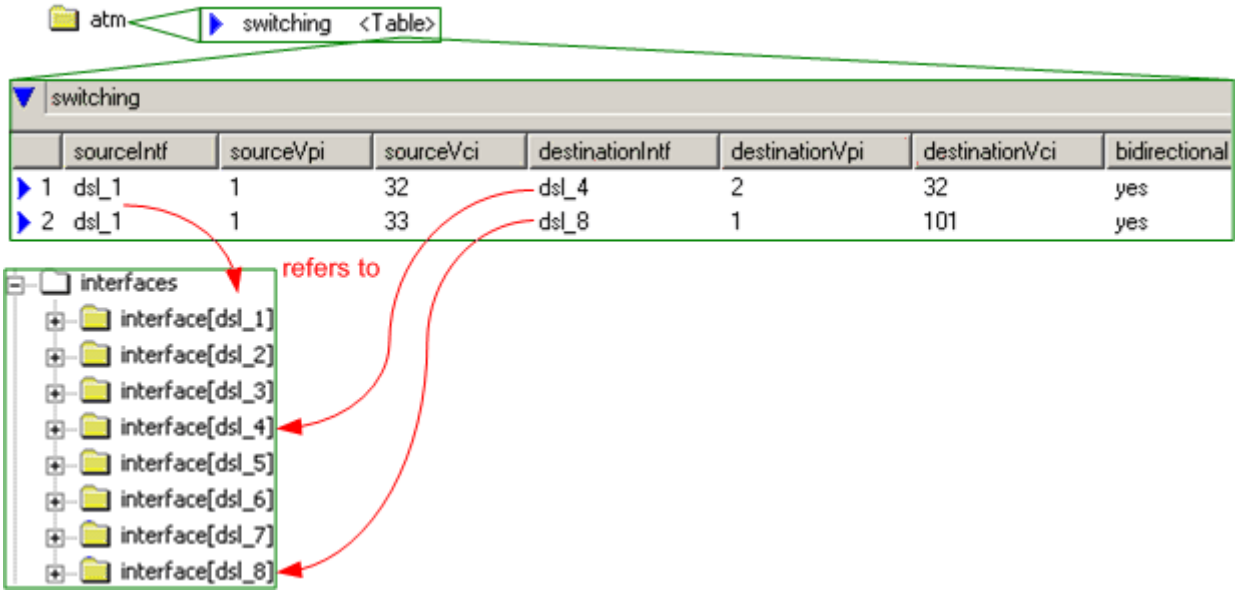
Step	Action
3	Configure the elements of the switching table: • sourceIntf. Use this element to enter the name of the (physical) source interface which carries the VC/VP that has to be switched. • sourceVpi. Use this element to enter the VPI of the VC/VP that has to be switched. • sourceVci. Use this element to enter the VCI of the VC that has to be switched. In case of VP switching, leave this element to its default value (<Opt>). Refer to What is VP switching? on page 257. • destinationIntf. Use this element to enter the name of the (physical) destination interface which carries the VC/VP when it has been switched. • destinationVpi. Use this element to enter the new VPI of the VC/VP when it has been switched. • destinationVci. Use this element to enter the new VCI of the VC when it has been switched. In case of VP switching, leave this element to its default value (<Opt>). • bidirectional. Use this element to determine whether the switching happens in both directions (bidirectional, i.e. from source to destination and vice versa) or only in one direction (unidirectional, i.e. only from source to destination). Refer to telindus24xx/atm/switching on page 399 for more information on the elements of the switching configuration attribute.

Example - configuring ATM switching

The following figure shows an xDSL line carrying 2 ATM PVCs that are switched to two separate xDSL lines:



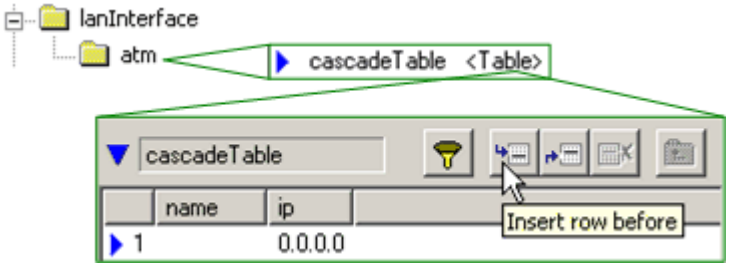
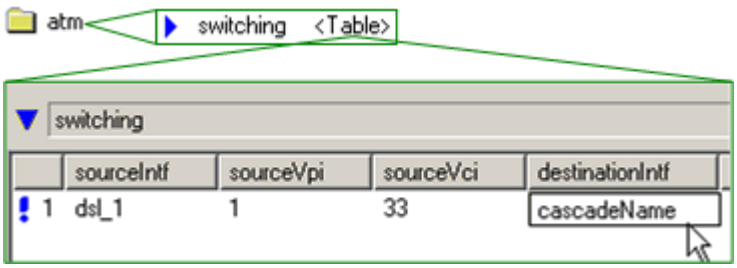
The following figure shows how to configure the ATM switching table.



11.3.3 How to cascade ATM switches?

Refer to 11.3.1 - Introducing ATM switching on page 257 for an introduction.

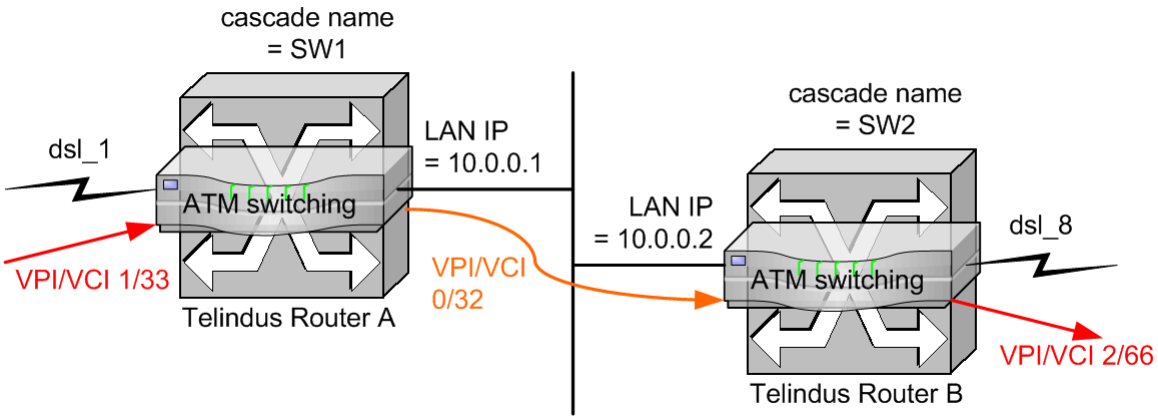
To configure the cascading of ATM switches, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the lanInterface/atm object, select the cascadeTable attribute and add one or more entries to this table.  Use this attribute to specify to which ATM switch you want to cascade. Add a row to the cascadeTable for each ATM switch you want to cascade to.
2	Configure the elements of the cascadeTable: • name. Use this element to associate a name with the IP address you have to enter in the ip element. This name has to be used in the ATM switching table in case you want to cascade an ATM PVC from this ATM switch to another ATM switch. • ip. Use this element to enter the LAN IP address of the ATM switch you want to cascade to. Refer to telindus24xx/lanInterface/atm/cascadeTable on page 321 for more information on the elements of the cascadeTable configuration attribute.
3	In the Telindus 2400 containment tree, go to the atm object and select the switching attribute. For all the ATM PVCs that you want to cascade from this ATM switch to another ATM switch, enter the name you specified in the cascadeTable as value of the destinationIntf element. 

Example - cascading ATM switches

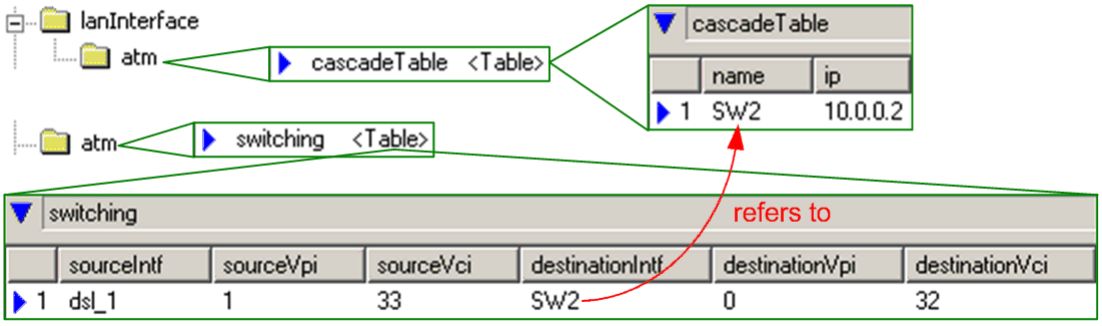
Suppose …

- you have two Telindus 2400s configured for ATM switching.
- one Telindus 2400 has LAN IP address 10.0.0.1 and cascade name SW1.
- one Telindus 2400 has LAN IP address 10.0.0.2 and cascade name SW2.
- you want to switch an ATM PVC on xDSL line 1 of ATM switch 1 to an ATM PVC on xDSL line 8 of ATM switch 2.

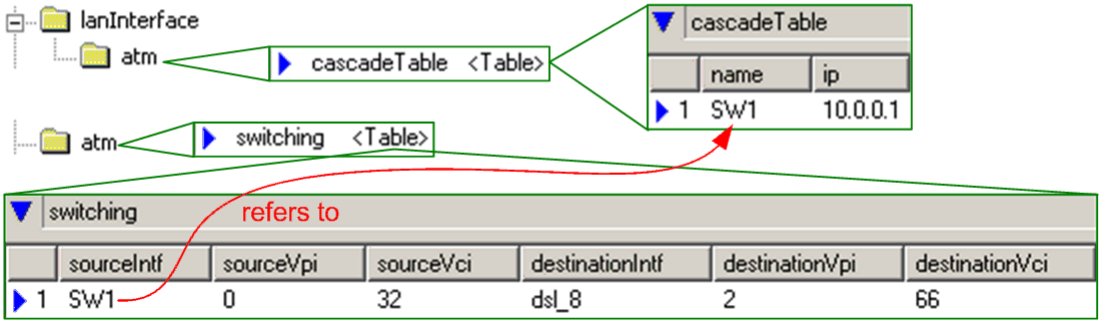


The following figure shows how to configure the ATM switching table and the cascade table of the two switches:

Telindus Router A :



Telindus Router B :



12 Configuring the additional features

This chapter introduces the most important additional features of the Telindus 2400 besides routing, bridging and switching and lists the attributes you can use to configure these features.

The following gives an overview of this chapter:

- 12.1 - Configuring DHCP on page 266
- 12.2 - Configuring an extended access list on page 271
- 12.3 - Configuring VLANs on page 278
- 12.4 - Configuring L2TP tunnels on page 282
- 12.5 - Configuring IP security on page 289

Refer to the Reference manual on page 295 for a complete overview of the attributes of the Telindus 2400.

12.1 Configuring DHCP

This section introduces the Dynamic Host Configuration Protocol (DHCP) and gives a short description of the attributes you can use to configure DHCP.

The following gives an overview of this section:

- 12.1.1 - Introducing DHCP on page 267
- 12.1.2 - Assigning static IP addresses on page 268
- 12.1.3 - Assigning dynamic IP addresses on page 269
- 12.1.4 - Configuring the Telindus 2400 as DHCP relay agent on page 270

12.1.1 Introducing DHCP

What is DHCP?

The DHCP protocol is a protocol for assigning IP addresses to devices on a network. DHCP can assign dynamic or static IP addresses. With dynamic addressing, a device can have a different IP address every time it connects to the network. What is more, the IP address can even change while the device is still connected.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

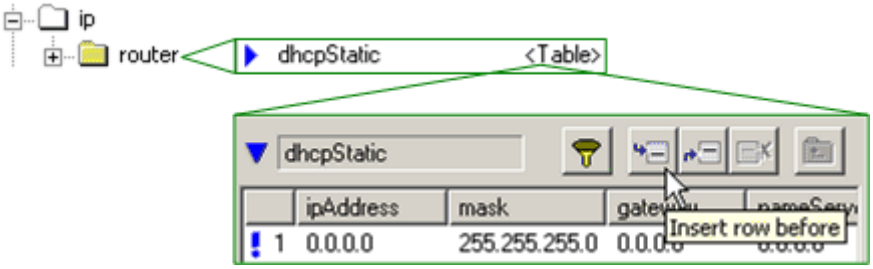
What is a DHCP relay agent?

Being a broadcast message, a DHCP request can not pass a router by default. To help a DHCP request pass the router, IP helper addresses have to be configured. This adds additional information to the request packets allowing servers on distant networks to send back the answer.

12.1.2 Assigning static IP addresses

Refer to 12.1.1 - Introducing DHCP on page 267 for an introduction.

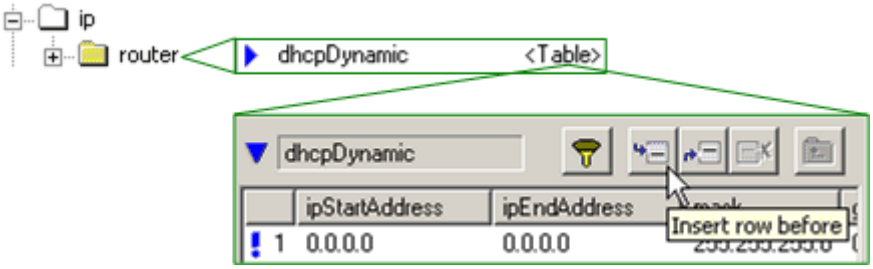
To assign static IP addresses to an IP device, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object, select the dhcpStatic attribute and add one or more entries to this table.  Use this attribute to assign a fixed IP address to an IP device and this for an infinite time. Add a row to the dhcpStatic table for each IP address you want to assign.
2	Configure the elements of the dhcpStatic table. The most important are: • ipAddress. Use this element to assign an IP address to a certain client. This client is identified with its MAC address. • mask. Use this element to set the client its subnet mask. • gateway. Use this element to set the default gateway for the client its subnet. • macAddress. Use this element to enter the client its MAC address. Refer to telindus24xx/ip/router/dhcpStatic on page 412 for more information.

12.1.3 Assigning dynamic IP addresses

Refer to 12.1.1 - Introducing DHCP on page 267 for an introduction.

To assign dynamic IP addresses to an IP device, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object, select the dhcpDynamic attribute and add one or more entries to this table.  Use this attribute to assign an IP address selected from an IP address range to an IP device and this for a certain time. Add a row to the dhcpDynamic table for each IP address range you want to create.
2	Configure the elements of the dhcpDynamic table. The most important are: • ipStartAddress. Use this element to define the start address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. • ipEndAddress. Use this element to define the end address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. • mask. Use this element to set the client its subnet mask for the specified IP address range. • gateway. Use this element to set the default gateway for the client its subnet. • leaseTime. Use this element to set the maximum time a client can lease an IP address from the specified IP address range. If 00000d 00h 00m 00s (default) is specified, then the lease time is infinite. Refer to telindus24xx/ip/router/dhcpDynamic on page 413 for more information.

12.1.4 Configuring the Telindus 2400 as DHCP relay agent

Refer to 12.1.1 - Introducing DHCP on page 267 for an introduction.

To configure the Telindus 2400 as DHCP relay agent, proceed as follows:

Step	Action
1	Specify (a) helper IP address(es) using the helpers element in the ip structure. Refer to 6.2.3 - Explaining the ip structure on page 90 for more information.
2	Now specify the helper protocols. By default, the helperProtocols table is empty. In this case the BootP/DHCP requests (among others) are forwarded automatically. However, specifying at least one value in the helperProtocols table clears the default helper list automatically. In that case you explicitly have to enter the BootP/DHCP protocol in the helperProtocols table. Refer to telindus24xx/ip/router/helperProtocols on page 409 for more information.

12.2 Configuring an extended access list

This section explains how to set up an extended access list. First it gives some general information on how extended access lists are implemented on the Telindus 2400. Then it shows how to set up and configure an extended access list.

- 12.2.1 - Introducing extended access lists on page 272
- 12.2.2 - Setting up an extended access list on page 273
- 12.2.3 - Configuring an extended access list on page 274

12.2.1 Introducing extended access lists

What is an extended access list?

Access lists control the access to or from an interface (LAN and/or WAN) for a number of specified services or IP addresses. The access list describes the condition to forward (permit) packets to an interface or to drop (deny) them.

Access lists are effective in one direction only, i.e. on the outgoing traffic of the interface:

- traffic from WAN to LAN is controlled by an access list on the LAN interface.
- traffic from LAN to WAN is controlled by an access list on the WAN interface.
- traffic from WAN to WAN is controlled by an access list on the outgoing WAN interface.

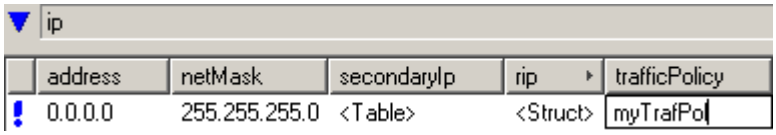
When access lists are combined with NAT/PAT translation, then first the conditions of the access list are applied before the NAT/PAT translation is done.

On the Telindus 2400, the extended access lists are implemented on both LAN and WAN interfaces using the traffic policy function and by defining traffic shaping rules.

12.2.2 Setting up an extended access list

This section explains how to set up an extended access list. 12.2.3 - Configuring an extended access list on page 274, explains how to configure the access list. I.e. how to define the filter criteria.

In order to set up an extended access list, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the profiles/policy/traffic object and add an ipTrafficPolicy[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56). E.g. ipTrafficPolicy[myTrafPol]
2	Go to the ip attribute of the interface on which you want to apply your extended access list. Example: Suppose you want to apply an extended access list on the LAN interface, then go to lanInterface object and then go to the ip attribute.
3	In the ip attribute, enter the index name of the ipTrafficPolicy[ ] object you created in step 1 as value of the trafficPolicy element. Example: In our example, enter the string myTrafPol as value of the trafficPolicy element. 
4	Go to the ipTrafficPolicy[ ] object you created in step 1 and make sure that the configuration attribute method is set to trafficShaping (this is the default value).
5	Configure the configuration attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping to match you filter criteria. Refer to 12.2.3 - Configuring an extended access list on page 274.

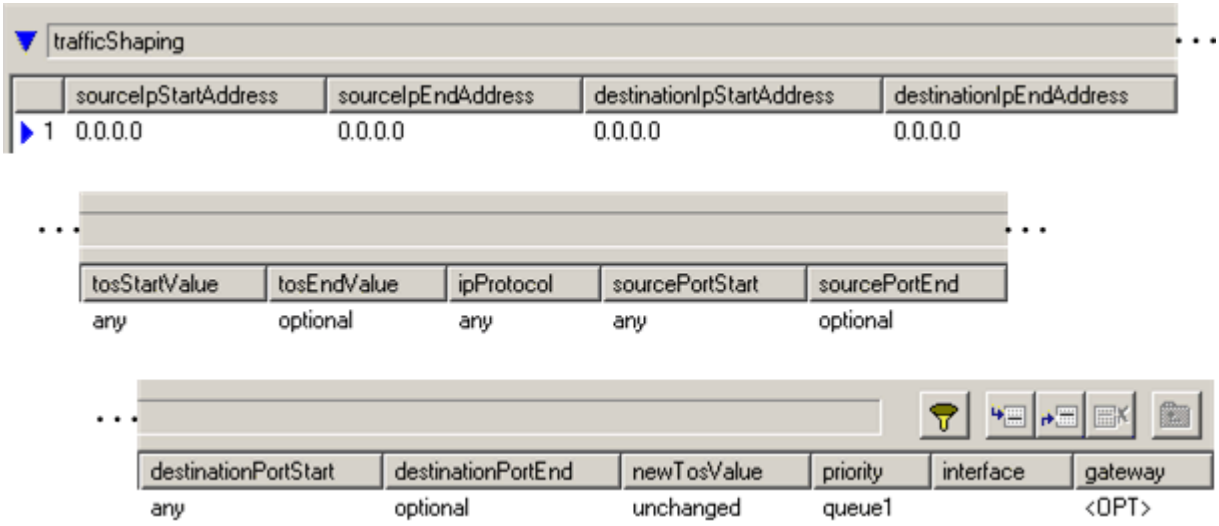
12.2.3 Configuring an extended access list

Whereas 12.2.2 - Setting up an extended access list on page 273 shows you how to set up an extended access list, this section shows you how to configure the access list. I.e. how to define the filter criteria.

You have to define your filter criteria in the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping attribute. This is a table, which is empty by default, but to which you can add several lines (entries).

- Once an entry is made in the trafficShaping table, only the traffic defined in the table is permitted. All other traffic is denied.
- If more than one entry applies to the same packet, then the entry which has the narrowest filter range (when looking at the filter criteria from left to right) is chosen. For example: two rows in the trafficShaping table apply to the same packet, but row 1 wants to forward packets to queue 3 and row 2 wants to forward packets to the low delay queue. In that case, first the IP source address is considered. The row with the smallest range wins. If the ranges are exactly the same, then the IP destination address is considered. And so on. Should the two rows be completely identical except for the queue, then one of the rows is chosen at random.

The following shows a screenshot of the trafficShaping table containing one line:



As you can see from the elements in the trafficShaping table, you can filter on several criteria:

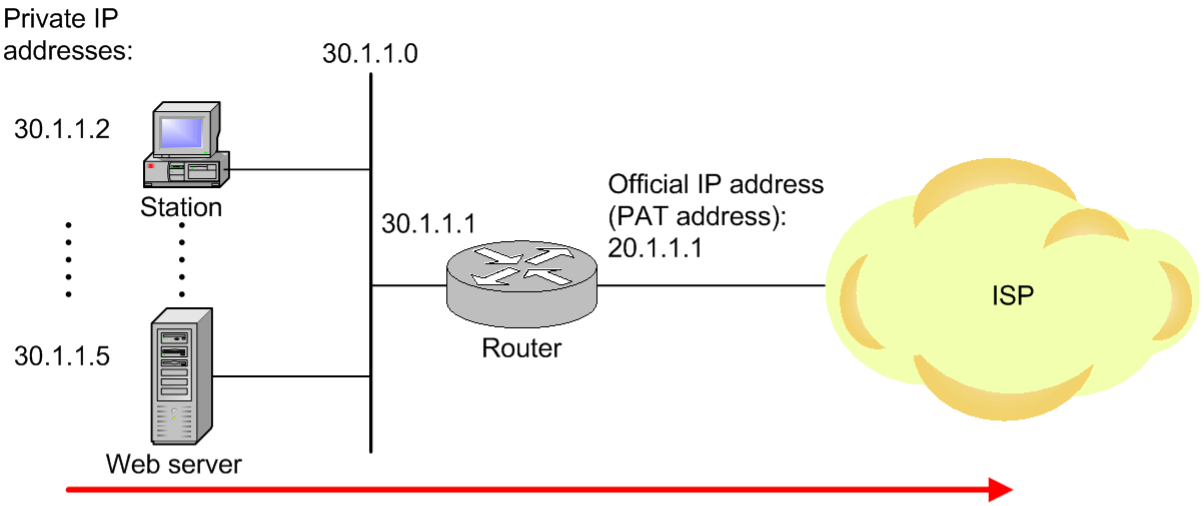
Filter criterion	Description
IP addresses	• 1 IP address: enter an IP address in the element sourceIpStartAddress and/or destinationIpStartAddress. • IP address range: enter an IP address range using the elements … - sourceIpStartAddress and sourceIpEndAddress and/or - destinationIpStartAddress and destinationIpEndAddress So if you define 1 or more IP addresses in the trafficShaping table, then traffic from (source) or to (destination) these IP addresses is allowed. All other traffic is discarded.

Filter criterion	Description
IP protocol	Specify an IP protocol using the ipProtocol element. Either select one of the common IP protocols from the ipProtocol element its drop-down box, or directly type a specific protocol number in the ipProtocol element field. So if you define an IP protocol in the trafficShaping table, then traffic carrying this IP protocol is allowed. All other traffic is discarded.
port number	• 1 port number: enter a port number in the element sourcePortStart and/or destinationPortStart. • port number range: enter a port number range using the elements … - sourcePortStart and sourcePortEnd and/or - destinationPortStart and destinationPortEnd So if you define 1 or more port numbers in the trafficShaping table, then traffic carrying these port numbers is allowed. All other traffic is discarded.
Type Of Service (TOS) value	• 1 TOS value: enter a TOS value in the element tosStartValue. • TOS value range: enter a TOS value range using the elements tosStartValue and tosEndValue. So if you define 1 or more TOS values in the trafficShaping table, then traffic carrying these TOS values is allowed. All other traffic is discarded.

Example - configuring an extended access list

This is an example of a network connected to the Internet and for which the following conditions are required:

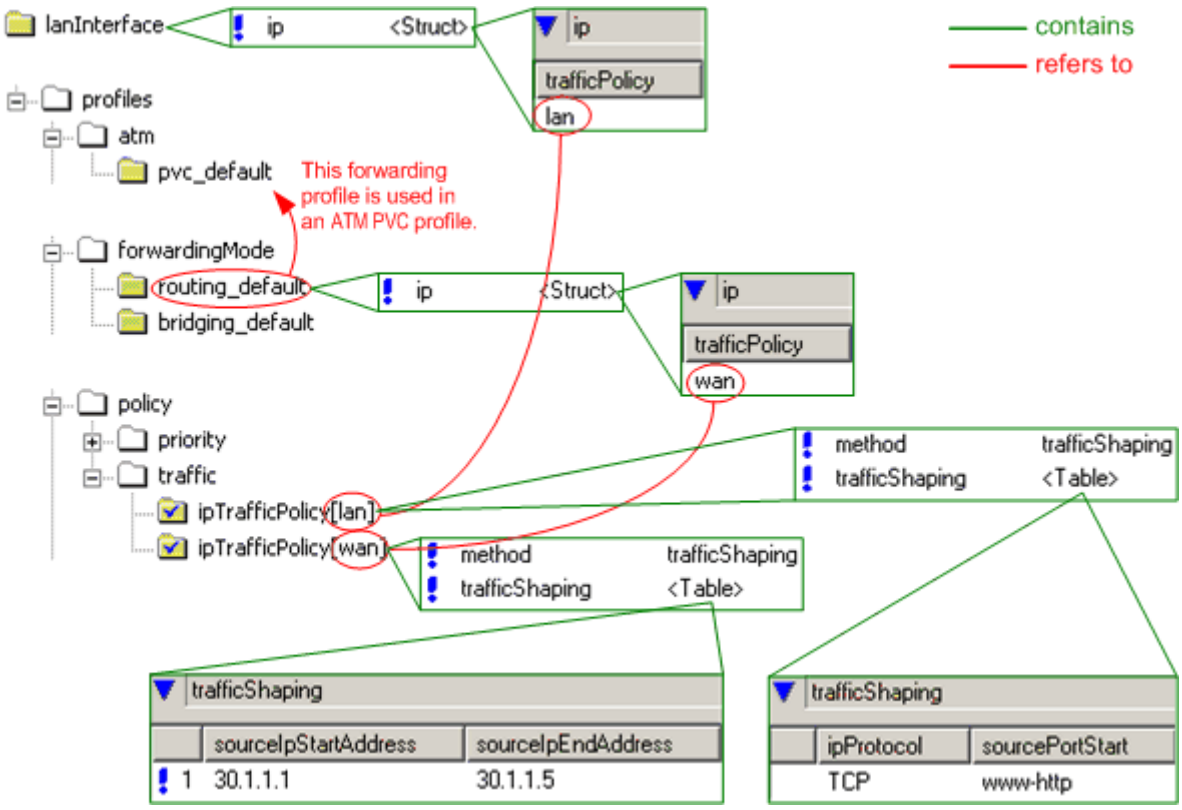
- only 5 stations may have access to the Internet.
- only the HTTP-port for web browsing is open for incoming packets from the Internet.



The access list on the WAN interface (refer to the trafficPolicy[wan] object) filters outgoing traffic. Only the stations with IP addresses 30.1.1.1 up to 30.1.1.5 are allowed to access the Internet.	PAT : the source IP address 30.1.1.x is changed to 20.1.1.1 and the source port is changed to a free port.	To the WAN interface.

To the LAN interface.	The access list on the LAN interface (refer to the trafficPolicy[lan] object) filters incoming traffic. Only port number 80 (www-http) is allowed.

The following figure shows how to configure the extended access lists:



12.3 Configuring VLANs

This section introduces VLANs and gives a short description of the attributes you can use to configure VLANs.

The following gives an overview of this section:

- 12.3.1 - Introducing VLANs on page 279
- 12.3.2 - Creating a VLAN on page 280

12.3.1 Introducing VLANs

Important remark

You can not create VLANs on the LAN interface and perform VLAN switching (refer to 11.2 - Configuring VLAN switching on page 251) at the same time. So either you create VLANs on the LAN interface, or either you perform VLAN switching.

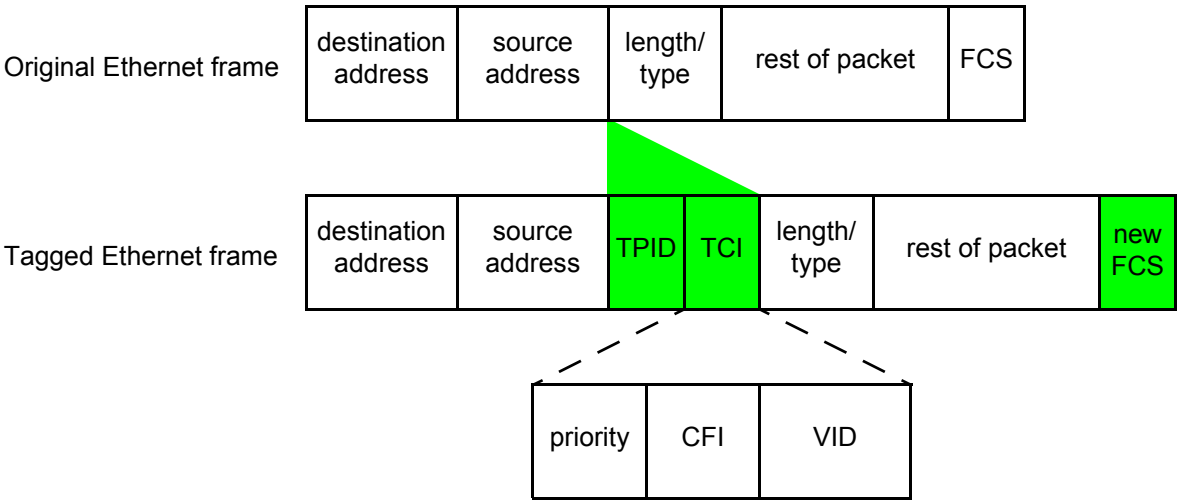
What is a VLAN?

A Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

What is a VLAN tag?

The VLAN tag header is inserted immediately following the destination MAC address and source MAC address fields of the frame. The VLAN tag header can be divided into two components:

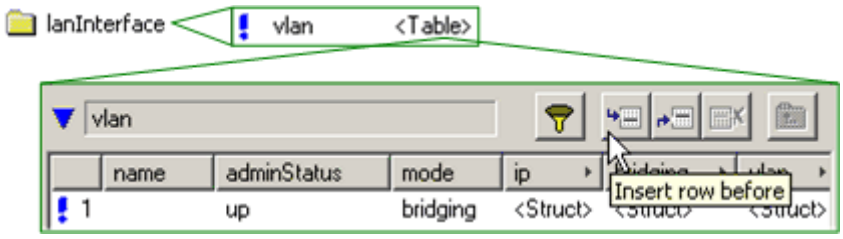
- TPID (Tag Protocol Identifier). The 802.1Q Ethernet-encoded TPID is defined as two octets with the value “8100”.
- TCI (Tag Control Information). The TCI field is also two octets in length and contains:
  - User priority. The user priority bits represents eight priority levels, 0 through 7. IEEE 802.1P defines the operation for these 3 user priority bits.
  - CFI (Canonical Format Indicator). The CFI bit indicates that all MAC address information carried by the frame that may be present in the MAC data is in Canonical format.
  - VID (VLAN Identifier). The twelve-bit VID field identifies the VLAN to which the frame belongs. Three VID values are reserved by the 802.1Q standard.



12.3.2 Creating a VLAN

Refer to 12.3.1 - Introducing VLANs on page 279 for an introduction.

To create a VLAN, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the lanInterface object, select the vlan attribute and add one or more entries to this table.  Use this attribute to configure the VLANs you want to set up. Add a row to the vlan table for each VLAN you want to set up. As long as no VLANs are created in the vlan table, the LAN interface accepts both VLAN untagged and VLAN tagged frames. The VLAN *untagged* frames are bridged and/or routed (depending on the setting of the mode attribute). The VLAN *tagged* frames are bridged (in case the mode attribute is set to bridging or bridgingAndRouting, else they are discarded). As soon as a VLAN is created in the vlan table, the LAN interface still accepts VLAN untagged frames but only accepts those VLAN tagged frames of which the VLAN ID corresponds with the VLAN ID that has been configured in the vlan table (see the vid element below). Other VLAN tagged frames are discarded.
2	Configure the elements of the vlan table: • name. Use this element to assign an administrative name to the VLAN. • adminStatus. Use this element to activate or deactivate the VLAN. • mode. Use this element to determine whether for the corresponding VLAN, IP packets are treated by the routing process or the bridging process. • ip. Use this element to configure the IP related parameters of the VLAN. Refer to 6.2.3 - Explaining the ip structure on page 90 for more information. • bridging. Use this element to configure the bridging related parameters in case the mode attribute is set to bridging. Refer to 10.2.6 - Explaining the bridging structure on page 241 for more information. • vlan. Use this element to configure the specific VLAN related parameters of the VLAN. See below. Refer to telindus24xx/lanInterface/vlan on page 316 for more information.

Step	Action
3	Configure the vlan structure in the vlan table. The elements in this structure are: • vid. Use this element to set the VLAN ID. • tagSignificance. Use this element to determine whether the VLAN tag has a local or a global significance. This element is only relevant when you set the mode element to bridging. If the tagSignificance is set to … - local, then the VLAN header is only relevant for the VLAN itself. When receiving a packet on the VLAN, the VLAN header is stripped before the packet is forwarded to the bridging engine. When transmitting a packet on the VLAN, the VLAN header is inserted. - global, then the VLAN header is not changed when forwarding packets. When connecting 2 or more Ethernet VLANs in the same bridge group, then make sure you set the tagSignificance to local, as both VLANs use different VLAN IDs. Refer to telindus24xx/lanInterface/vlan/vlan on page 317 for more information.

12.4 Configuring L2TP tunnels

This section introduces the Layer 2 Tunnelling Protocol (L2TP) and gives a short description of the attributes you can use to configure L2TP.

The following gives an overview of this section:

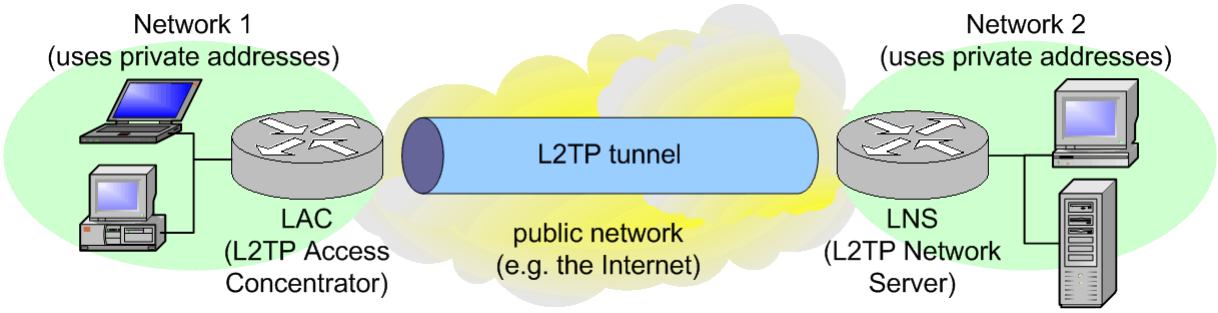
- 12.4.1 - Introducing L2TP tunnels on page 283
- 12.4.2 - Setting up an L2TP tunnel on page 285
- 12.4.3 - How does an L2TP tunnel work? on page 288

12.4.1 Introducing L2TP tunnels

What is an L2TP tunnel?

The Layer 2 Tunnelling Protocol (L2TP) is a protocol used for connecting VPNs (Virtual Private Networks) over public lines. More specific, it allows you to set up virtual PPP connections. In other words, an L2TP tunnel simulates an additional PPP interface which directly connects two routers with each other.

Concrete, using the Layer 2 Tunnelling Protocol you can connect several private and physically dispersed local networks with each other over public lines (such as the Internet) in order to create one big (virtual) local network. This without the need for address translation.



L2TP tunnel terminology

The following table gives some specific L2TP terminology:

Term	Description
L2TP Access Concentrator (LAC)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Network Server (LNS). Packets sent from the LAC to the LNS require tunnelling with the L2TP protocol.
L2TP Network Server (LNS)	A node that acts as one side of an L2TP tunnel. It is a peer to the L2TP Access Concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunnelled from the remote system by the LAC.
Tunnel	A tunnel exists between a LAC-LNS pair. The tunnel consists of a Control Connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and Control Messages between the LAC and the LNS.
Control Connection	A control connection operates in-band over a tunnel to control the establishment, release, and maintenance of sessions and of the tunnel itself.
Control Messages	Control messages are exchanged between LAC and LNS pairs, operating in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.

L2TP tunnel encapsulation

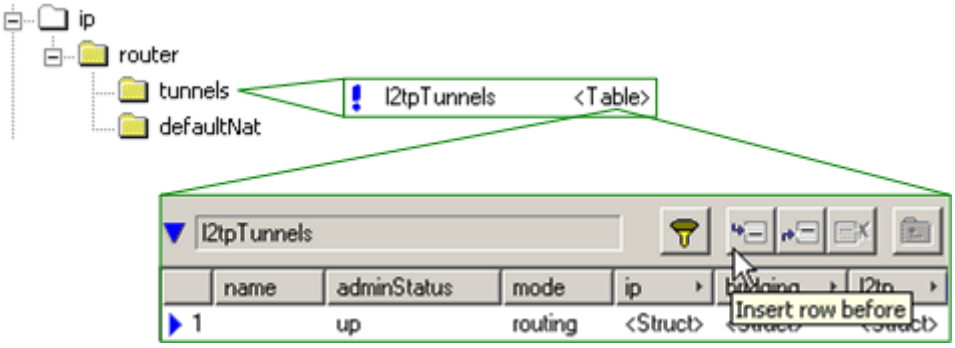
The following table shows the L2TP encapsulation on the LAN and WAN interface:

<table>
<tr><th>Interface</th><th>L2TP encapsulation</th></tr>
<tr><td>WAN interface</td><td>The L2TP encapsulation on the WAN interface is as follows:
<table><tr><td>PPP
FR
AAL5</td><td>IP</td><td>UDP</td><td>L2TP</td><td>PPP</td><td>IP
Ethernet</td><td>…</td></tr></table></td></tr>
<tr><td>LAN interface</td><td>The L2TP encapsulation on the LAN interface is as follows:
<table><tr><td>MAC</td><td>IP</td><td>UDP</td><td>L2TP</td><td>PPP</td><td>IP
Ethernet</td><td>…</td></tr></table></td></tr>
</table>

12.4.2 Setting up an L2TP tunnel

Refer to 12.4.1 - Introducing L2TP tunnels on page 283 for an introduction.

To set up an L2TP tunnel, proceed as follows:

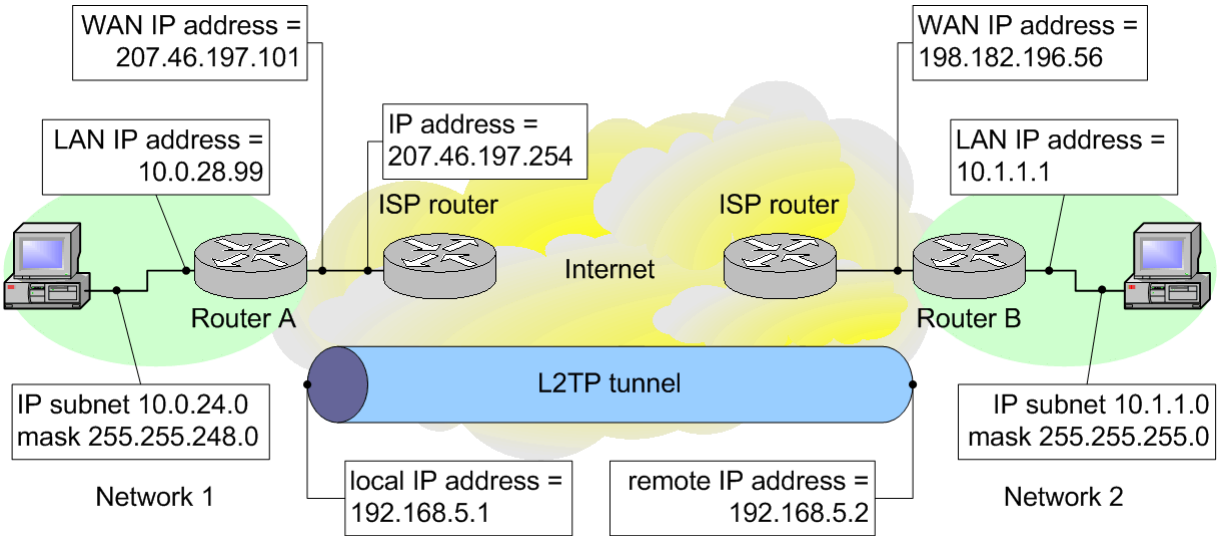
Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router/tunnels object, select the l2tpTunnels attribute and add one or more entries to this table.  Use this attribute to configure the Layer 2 Tunnelling Protocol tunnels you want to set up. Add a row to the l2tpTunnels table for each L2TP tunnel you want to set up.
2	Configure the elements of the l2tpTunnels table: • name. Use this element to assign an administrative name to the tunnel. • adminStatus. Use this element to activate or deactivate the tunnel . • mode. Use this element to determine whether for the corresponding tunnel, IP packets are treated by the routing process, the bridging process or both. • ip. Use this element to configure the IP related parameters of the tunnel. Building an L2TP tunnel is based on logical interfaces. Those logical interfaces have their own IP address. Refer to 6.2.3 - Explaining the ip structure on page 90 for more information. • bridging. Use this element to configure the bridging related parameters in case the mode attribute is set to bridging or routingAndBridging. Refer to 10.2.6 - Explaining the bridging structure on page 241 for more information. • l2tp. Use this element to configure the L2TP related parameters of the tunnel. See below. Refer to telindus24xx/ip/router/tunnels/l2tpTunnels on page 431 for more information.
3	Configure the l2tp structure in the l2tpTunnels table. The most important elements in this structure are: • localIpAddress. Use this element to set the IP address that serves as start point of the L2TP tunnel. • remoteIpAddress. Use this element to set the IP address that serves as end point of the L2TP tunnel. • type. Use this element to specify the tunnel type (incoming or outgoing). • mode. Use this element to set the L2TP mode of the Telindus 2400 (LAC, LNS or auto). Only use auto in case a Telindus router is located at *both sides* of the tunnel. Refer to telindus24xx/ip/router/tunnels/l2tpTunnels/l2tp on page 433 for more information.

Remarks

- L2TP tunnels can also be set up by an IP host. The Telindus 2400 is transparent for tunnels set up by a host.
- Multiple L2TP tunnels are possible on a single link. Multiple PPP sessions are possible within a single L2TP tunnel.

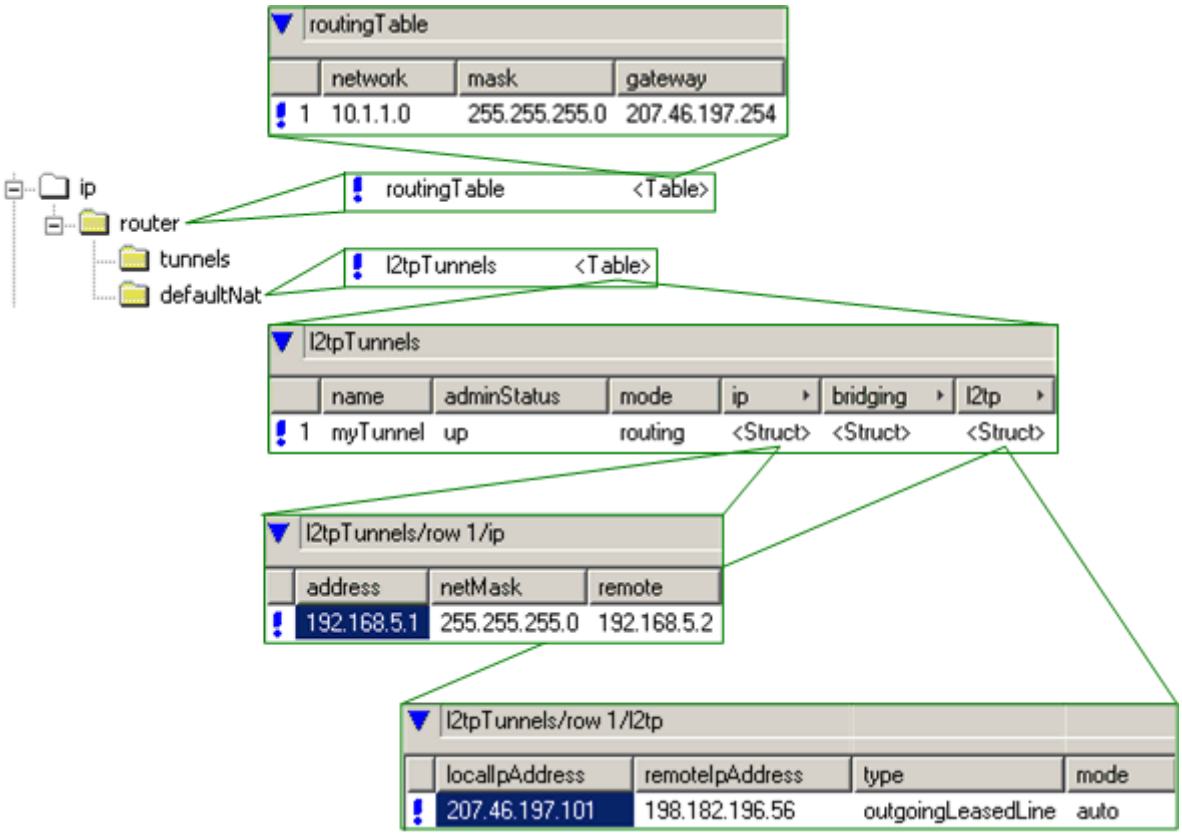
Example - configuring an L2TP tunnel

Suppose private network 1 has to be interconnected to private network 2 over the Internet. For this purpose you want to set up an L2TP tunnel between the two access routers of these private networks.



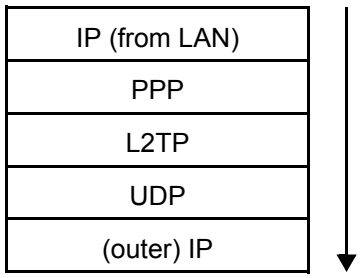
So first create a route between the WAN interfaces of Router A and B. Then set up the tunnel between the WAN interfaces of Router A and B (i.e. the tunnel start point is IP address 207.46.197.101, the tunnel end point is IP address 198.182.196.56).

The following figure shows how to set up the L2TP tunnel:



12.4.3 How does an L2TP tunnel work?

Suppose a packet coming from the LAN has a destination address for a network that is accessible through an L2TP tunnel. The following happens:

Phase	Description
1	The packet goes through the routing decision process. If the result of this decision is a route which uses the tunnel interface, then the packet is encapsulated in PPP first, then L2TP, UDP and finally IP. 
2	Then the packet goes through the routing decision process again. This time using the outer IP header.
3	The packet is routed over the Internet using the outer IP header.
4	The packet is received in the tunnel's end point, where it is then routed again using the original IP header.

12.5 Configuring IP security

This section introduces the IP security (IPSEC) and gives a short description of the attributes you can use to configure IPSEC.

The following gives an overview of this section:

- 12.5.1 - Introducing IPSEC on page 290
- 12.5.2 - Setting up an IPSEC secured L2TP tunnel on page 292

12.5.1 Introducing IPSEC

What is IPSEC?

IPSEC (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSEC is deployed widely to implement Virtual Private Networks (VPNs). A big advantage of IPSEC is that security arrangements can be handled without requiring changes to individual user computers.

The IPSEC security services (ESP and AH)

IPSEC provides two choices of security service:

- Authentication Header (AH), essentially allows authentication of the sender of data. AH is not supported by the Telindus 2400.
- Encapsulating Security Payload (ESP), which is supported by the Telindus 2400, allows both authentication of the sender and encryption of data as well.

The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

The IPSEC modes

IPSEC features two basic modes: transport mode or tunnel mode. The Telindus 2400 currently supports L2TP transport mode. I.e. traffic destined for an L2TP tunnel is secured with IPSEC (refer to RFC 3193, Securing L2TP using IPSEC).

What is a security association (SA)?

IPSEC provides different options for performing network encryption and authentication. The two communicating nodes must determine exactly which algorithms to use (e.g. DES or 3DES for encryption, MD5 or SHA for integrity and authentication) and must share session keys.

All this information is described in the Security Association (SA). In other words, the security association is simply a statement of the negotiated security policy between two devices.

There are two types of security associations:

- Manual SA
- Dynamic SA

The Telindus 2400 currently supports Manual SA. This requires no negotiation. All values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place.

In principle, security association is unidirectional (half-duplex). I.e. one SA for the inbound traffic and one SA for the outbound traffic. The Telindus 2400 also supports full-duplex SA (one SA for both inbound and outbound traffic).

IPSEC encryption

When using ESP, you can encrypt the data using the Data Encryption Standard (DES or 3DES).

DES is a widely-used method of data encryption using a private (secret) key. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. Triple DES applies three keys in succession.

IPSEC authentication

When using ESP, you can not only encrypt but also authenticate the data using the Keyed-Hashing for Message Authentication (HMAC).

HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key.

What is the Security Parameter Index (SPI)?

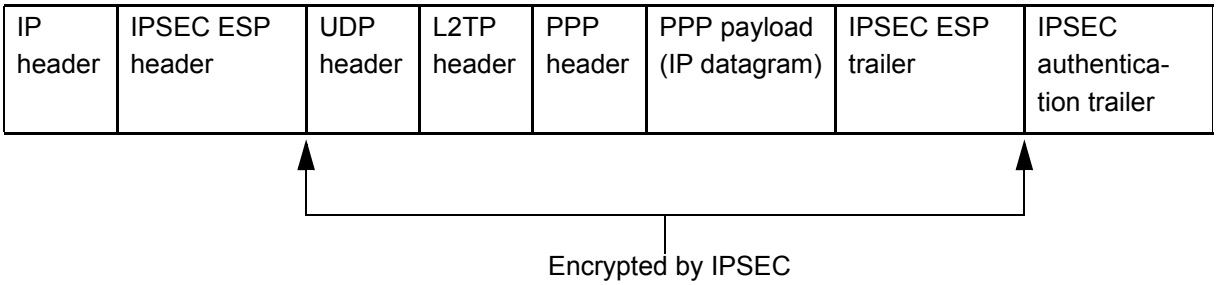
An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.

IPSEC compatibility

IPSEC on the Telindus 2400 is compatible with IPSEC on Cisco devices and on Linux.

IPSEC encapsulation

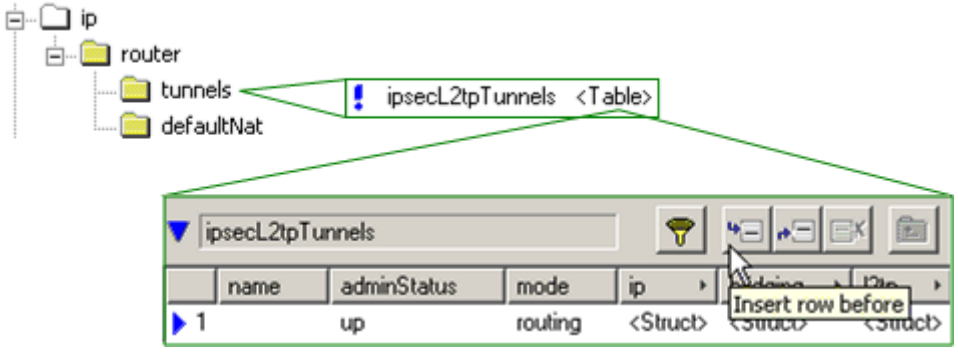
The following shows the IPSEC encapsulation:

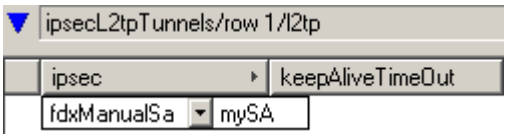


12.5.2 Setting up an IPSEC secured L2TP tunnel

Refer to 12.5.1 - Introducing IPSEC on page 290 for an introduction.

In order to set up an L2TP tunnel secured with IPSEC, proceed as follows:

Step	Action
1	In the Telindus 2400 containment tree, go to the ip/router object and add a manualSA[ ] object underneath (refer to 4.4 - Adding an object to the containment tree on page 56). E.g. manualSA[mySA]
2	Now configure the attributes of the manualSA[ ] object you added in step 1 to your needs. These attribute are: • espEncryptionAlgorithm. Use this attribute to select the algorithm that will be used to encrypt the data when using IPSEC. • espEncryptionKey. Use this attribute to define the key that will be used in the encryption / decryption process when using IPSEC. • espAuthenticationAlgorithm. Use this attribute to select the algorithm that will be used to authenticate the data when using IPSEC. • espAuthenticationKey. Use this attribute to define the key that will be used in the authentication process when using IPSEC. • spi. Use this attribute to set the SPI value. Each security association must have a unique SPI value because this value is used to identify the security association. Refer to 13.12.4 - Manual SA configuration attributes on page 438 for more information.
3	In the Telindus 2400 containment tree, go to the ip/router/tunnels object, select the ipsecL2tpTunnels attribute and add one or more entries to this table.  Use this attribute to configure the IP secured Layer 2 Tunnelling Protocol tunnels you want to set up. Add a row to the IpsecL2tpTunnels table for each IPSEC L2TP tunnel you want to set up.
4	Configure the non-IPSEC related parameters in the ipsecL2tpTunnels table as described in 12.4.2 - Setting up an L2TP tunnel on page 285. The only IPSEC related parameter is the ipsec element in the l2tp structure of the ipsecL2tpTunnels table.

Step	Action
5	Go to the l2tp structure in the ipsecL2tpTunnels table and enter the index name of the manualSA[ ] object you added in step 1 as value of the ipsec element. By doing so, you apply the security association on the L2TP tunnel. Note that in the ipsec element you can choose between full-duplex or half-duplex manual SA (fdxManualSa or hdxManualSa). Refer to telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/l2tp/ipsec on page 436 for more information. E.g. in our example, enter the string mySA as value of the ipsec element. 

Reference manual

13 Configuration attributes

This chapter discusses the configuration attributes of the Telindus 2400. The following gives an overview of this chapter:

- 13.1 - Configuration attribute overview on page 298
- 13.2 - General configuration attributes on page 306
- 13.3 - LAN interface configuration attributes on page 312
- 13.4 - Cascading configuration attributes on page 320
- 13.5 - 4 port Ethernet interface configuration attributes on page 322
- 13.6 - 6E1 interface configuration attributes on page 323
- 13.7 - E3/T3 interface configuration attributes on page 333
- 13.8 - IMA group configuration attributes on page 349
- 13.9 - xDSL interface configuration attributes on page 352
- 13.10 - Profile configuration attributes on page 354
- 13.11 - ATM switching configuration attributes on page 398
- 13.12 - Router configuration attributes on page 400
- 13.13 - Bridge configuration attributes on page 445
- 13.14 - Alarm in contacts configuration attributes on page 456
- 13.15 - SNMP configuration attributes on page 459
- 13.16 - Management configuration attributes on page 461
- 13.17 - Loopback configuration attributes on page 470

13.1 Configuration attribute overview

Refer to 4.3 - The objects in the Telindus 2400 containment tree on page 52 to find out which objects are present by default, which ones you can add yourself and which ones are added automatically.

> telindus24xx
- sysName
- sysContact
- sysLocation
- bootFromFlash
- security
- masterClock
- alarmMask
- alarmLevel
- Action: Activate Configuration
- Action: Load Saved Configuration
- Action: Load Default Configuration
- Action: Cold Boot

>> lanInterface
- name
- mode
- ip
- arp
- bridging
- adapter
- vlan
- alarmMask
- alarmLevel
- alarmContactHighMask
- alarmContactLowMask

>>> atm
- cascadeTable

>> 4pEth
- name
- mode
- ip
- arp
- bridging
- vlan
- alarmMask
- alarmLevel

>> hexE1
- ifClocking
- imaVersion
- imaDifferentialDelay

>>> e1[E1_x]

- name
- coding
- crc4Insertion
- aisDetection
- sqThreshold
- sqTime
- alarmMask
- alarmLevel
- alarmContactHighMask
- alarmContactLowMask

>>>> atm

- atmConfig

>> e3T3

>>> e3T3[E3T3_x]

- ifClocking
- aisDetection
- sqThreshold
- sqTime
- alarmMask
- alarmLevel
- alarmContactHighMask
- alarmContactLowMask

>>>> atm

- pvc
- vp
- atmConfig

>> bundle

>>> imaGroup[ ]

- members
- minActiveLinks
- pvc
- vp
- txFrameLength
- rxFrameLength
- traceMessages

>> dslInterfaces

- ifClocking

>>> interface[dsl_x]

lineConfiguration
alarmMask
alarmLevel

>> profiles

>>> xdsl

>>>> shdsl_default[1]

region
mode
minSpeed
maxSpeed
minSpeed2P
maxSpeed2P
linkAlarmThresholds
retrain
management
lineAlarmMask
lineAlarmLevel
lineAlarmContactHighMask
lineAlarmContactLowMask
linePairAlarmMask
linePairAlarmLevel
linePairAlarmContactHighMask
linePairAlarmContactLowMask
repeaterAlarmMask
repeaterAlarmLevel
repeaterLinePairAlarmMask
repeaterLinePairAlarmLevel
endAlarmMask
endAlarmLevel
endLinePairAlarmMask
endLinePairAlarmLevel

1. Telindus 2400 SHDSL models only (2421, 2422, 2423).

>>>> adsl_default[2]

- standard
- usMinSpeed
- usMaxSpeed
- dsMinSpeed
- dsMaxSpeed
- retrain
- latency
- usInterleaveDelay
- dsInterleaveDelay
- usCorrectionTime
- dsCorrectionTime
- linkAlarmThresholds
- lineAlarmMask
- lineAlarmLevel
- lineAlarmContactHighMask
- lineAlarmContactLowMask
- linePairAlarmMask
- linePairAlarmLevel
- linePairAlarmContactHighMask
- linePairAlarmContactLowMask

>>> atm

>>>> pvc_default

- vpi
- vci
- qos
- higherLayerProtocol
- mode
- oamF5Loopback
- maxFifoQLen

>>> forwardingMode

>>>> routing_default

- ip
- priorityPolicy

>>>> bridging_default

- bridging
- priorityPolicy

2. Telindus 2400 ADSL models only (2401, 2402, 2403).

>>> policy

>>>> traffic

>>>>> ipTrafficPolicy[ ]
method
trafficShaping
tos2QueueMapping
dropLevels

>>>>> bridgingTrafficPolicy[ ]
vlanPriorityMap
dropLevels

>>>> priority

>>>>> priorityPolicy[ ]
algorithm
countingPolicy
queueConfigurations
lowDelayQuotum

>> configurations

>>> shdslAtm_default[3]
shdslProfile
pvc
vp

>>> adslAtm_default[4]
adslProfile
pvc
vp

>> atm
switching

3. Telindus 2400 SHDSL models only (2421, 2422, 2423).
4. Telindus 2400 ADSL models only (2401, 2402, 2403).

>> ip

>>> router

defaultRoute
routingTable
routingProtocol
alternativeRoutes
ripUpdateInterval
ripHoldDownTime
ripv2SecretTable
sysSecret
pppSecretTable
helperProtocols
sendTtlExceeded
sendPortUnreachable
sendAdminUnreachable
dhcpStatic
dhcpDynamic
dhcpCheckAddress
dns
radius
addrPools
alarmMask
alarmLevel

>>>> defaultNat

patAddress
portTranslations
servicesAvailable
addresses
gateway
tcpSocketTimeOut
udpSocketTimeOut
tcpSockets
udpSockets
dmzHost

>>>> tunnels

l2tpTunnels
ipsecL2tpTunnels

>>>> manualSA[ ]

espEncryptionAlgorithm
espEncryptionKey
espAuthenticationAlgorithm
espAuthenticationKey
spi

>>>> routingFilter[ ]
filter

>> bridge

>>> bridgeGroup
name
ip
arp
bridgeCache
bridgeTimeOut
spanningTree
localAccess
macAddress
vlan
vlanSwitching

>>> vpnBridgeGroup[ ]
ip
arp
bridgeCache
bridgeTimeOut
spanningTree
localAccess
macAddress
vlan
vlanSwitching

>>> accessList[ ]
macAddress

>> alarmContacts
alarmMask
alarmLevel
alarmContactHighMask
alarmContactLowMask

>> snmp
trapDestinations
mib2Traps

>> management

ctrlPortProtocol
sysLog
timeServer
timeZone
cms2Address
accessList
snmp
telnet
tftp
ftp
consoleNoTrafficTimeOut
alarmFilter
timedStatsAvailability
atwinGraphics

>>> loopback

ipAddress

13.2 General configuration attributes

This section describes the following configuration attributes:

- telindus24xx/sysName on page 307
- telindus24xx/sysContact on page 307
- telindus24xx/sysLocation on page 307
- telindus24xx/bootFromFlash on page 307
- telindus24xx/security on page 308
- telindus24xx/masterClock on page 309
- telindus24xx/<alarmConfigurationAttributes> on page 309

This section describes the following actions:

- telindus24xx/Activate Configuration on page 310
- telindus24xx/Load Default Configuration on page 310
- telindus24xx/Load Saved Configuration on page 311
- telindus24xx/Cold Boot on page 311

telindus24xx/sysName

Default:<empty>
Range: 0 … 64 characters

Use this attribute to assign a name to the Telindus 2400. This attribute is also used in the PPP authentication process. The PPP authenticator uses the sysName attribute in order to verify the peer its response.

For more information on PPP authentication, refer to …

- 7.2.6 - Configuring PAP on page 146
- 7.2.8 - Configuring CHAP on page 149

telindus24xx/sysContact

Default:<empty>
Range: 0 … 64 characters

Use this attribute to add contact information. You could, for instance, enter the name and telephone number of the person to contact in case problem occur.

telindus24xx/sysLocation

Default:<empty>
Range: 0 … 64 characters

Use this attribute to specify the physical location of the Telindus 2400.

telindus24xx/bootFromFlash

Default:auto
Range: enumerated, see below

Use this attribute to specify which application software version the Telindus 2400 has to use to operate from.

Part of the flash memory of the Telindus 2400 is organised as a file system. In this file system, you can store two complete application software versions. You can use the bootFromFlash attribute to switch between these softwares.

When you store two application software versions in the file system, they are automatically renamed as CONTROL1 and CONTROL2, respectively. You can check this with the status attribute telindus24xx/fileSystem/fileList.

The bootFromFlash attribute has the following values:

Value	When the Telindus 2400 boots …
flash1	the application software CONTROL1 is active.
flash2	the application software CONTROL2 is active.
auto	the Telindus 2400 automatically chooses the most recent application software. It does this by comparing the application software version numbers.

telindus24xx/security

Default:<empty>
Range: table, see below

Use this attribute to create a list of passwords with associated access levels in order to avoid unauthorised access to the Telindus 2400 and the network.

The security table contains the following elements:

Element	Description
password	Use this element to set the password. You can then associate this password with a certain access level. Default:<empty> Range: 0 … 10 characters
accessRights	Use this element to set the access level associated with the password. It is a bit string of which each bit corresponds to an access level. The different access levels are listed below. Default:11111 Range: bit string, see below

The following table shows, for each access level, what you can or can not do:

Access level	Read attributes	Change attributes	Read security attributes[1]	Change security attributes	Execute actions[2]	Access file system
readAccess	yes	no	no	no	no	no
writeAccess	yes	yes	no	no	no	no
securityAccess	no	no	yes	yes	no	no
fileSystem-Access	no	no	no	no	no	yes
testAccess	no	no	no	no	yes	no

1. The Telindus 2400 has the following security attributes:
   telindus24xx/sysName and security
   telindus24xx/profiles/policy/priority/priorityPolicy[ ]
   telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ] and bridgingTrafficPolicy[ ]
   telindus24xx/ip/router/sysSecret, pppSecretTable, ripv2SecretTable and radius
   telindus24xx/ip/router/tunnels, routingFilter[ ] and manualSA
   telindus24xx/management/accessList, snmp, telnet, tftp and ftp
2. Actions are e.g. Cold Boot, clearArpCache, clearBridgeCache, etc…

Important remarks

- If you create no passwords, everybody has complete access.
- If you define at least one password, it is impossible to access the Telindus 2400 with one of the management systems without entering the correct password.
- If you create a list of passwords, create at least one with write and security access. If not, you will be unable to make configuration and password changes after activation of the new configuration.

telindus24xx/masterClock

Default:internal
Range: enumerated, see below

Use this attribute to specify which clock has to be used as master clock (i.e. the clock that is used by the Telindus 2400 itself). Note that you can set the master clock and the TIM interface clock (in case a TIM interface is used) independently from each other (refer to the ifClocking attribute of the TIM interfaces).

The masterClock attribute has the following values:

Value	Description
internal	The master clock is generated internally by the Telindus 2400.
station	If a valid clock signal is present on the station clock connector (CLK), then this is used as master clock. Refer to 2.6.2 - Connecting the different parts of the Telindus 2400 on page 27, for the location of the station clock connector on the front panel.
ifModule	If a valid clock signal is coming from the TIM (Telindus Interface Module), then this is used as master clock. If you set the masterClock attribute to ifModule, then do not set the ifClocking attribute to masterClock, since this is an illegal configuration.

telindus24xx/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask and alarmLevel and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the telindus24xx object, refer to 16.3 - General alarms on page 649.

telindus24xx/Activate Configuration

If you execute this action, the editable non-active configuration becomes the active configuration. Refer to 6.6.1 - What are the different configuration types? on page 111 for more information.

When use this action?

If you configure the Telindus 2400 using …

- any other maintenance tool than the graphical user interface based TMA (e.g. ATWIN, CLI, Web Interface, EasyConnect terminal, TMA CLI), then execute the Activate Configuration action to activate the configuration after you finished configuring the Telindus 2400 or after you executed the Load Saved Configuration or Load Default Configuration action.
- TMA, then do not just execute the Activate Configuration action to activate the configuration after you finished configuring the Telindus 2400, but use the TMA button *Send all attributes to device* instead.
  You can, however, execute the Activate Configuration action after you executed the Load Saved Configuration or Load Default Configuration action.

telindus24xx/Load Default Configuration

If you execute this action, the non-active configuration is overwritten by the default configuration. Refer to 6.6.1 - What are the different configuration types? on page 111 for more information.

When use this action?

If you install the Telindus 2400 for the first time, all configuration attributes have their default values. If the Telindus 2400 has already been configured but you want to start from scratch, then use this action to revert to the default configuration.

In case of TMA, click on the TMA button *Retrieve all attributes from device* after executing the Load Default Configuration action to see the new non-active configuration.

telindus24xx/Load Saved Configuration

If you execute this action, the non-active configuration is overwritten by the active configuration currently used by the Telindus 2400. Refer to 6.6.1 - What are the different configuration types? on page 111 for more information.

When use this action?

If you are in the progress of modifying the non-active configuration but made some mistakes, then use this action to revert to the active configuration.

In case of TMA, click on the TMA button *Retrieve all attributes from device* after executing the Load Saved Configuration action to see the new non-active configuration.

telindus24xx/Cold Boot

If you execute this action, the Telindus 2400 reboots. As a result, the Telindus 2400 …

- performs a self-test.
- checks the software.
- reads the saved configuration and restarts program execution.

When use this action?

Use this action, for instance, to activate new application software.

13.3 LAN interface configuration attributes

This section describes the following configuration attributes:

- telindus24xx/lanInterface/name on page 313
- telindus24xx/lanInterface/mode on page 313
- telindus24xx/lanInterface/ip on page 313
- telindus24xx/lanInterface/arp on page 314
- telindus24xx/lanInterface/bridging on page 315
- telindus24xx/lanInterface/adapter on page 315
- telindus24xx/lanInterface/vlan on page 316
- telindus24xx/lanInterface/<alarmConfigurationAttributes> on page 319

telindus24xx/lanInterface/name

Default:lan
Range: 1 … 24 characters

Use this attribute to assign an administrative name to the LAN interface.

telindus24xx/lanInterface/mode

Default:bridging
Range: enumerated, see below

Use this attribute to determine whether the packets are treated by the routing process, the bridging process or both.

The mode attribute has the following values:

Value	Description
bridging	All packets are bridged. The settings of the IP configuration attributes of the LAN are ignored. If you want to manage the Telindus 2400 via IP, you have to configure an IP address in the bridgeGroup object. Refer to telindus24xx/bridge/bridgeGroup/ip on page 447.
routing	The IP packets are routed. All other protocols are discarded.
routingAndBridging	IP packets are routed. Non-IP packets are bridged. The settings of the IP configuration attributes of the LAN are taken into account.

telindus24xx/lanInterface/ip

Default:-
Range: structure, see below

Use this attribute to configure the IP related parameters of the LAN interface.

Refer to …

- 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses.
- 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.

Important remark

If you set the configuration attribute telindus24xx/lanInterface/mode to bridging, then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 2400 via IP, you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.

telindus24xx/lanInterface/arp

Default:-
Range: structure, see below

Use this attribute to configure the Address Resolution Protocol (ARP) cache.

The arp structure contains the following elements:

Value	Description	
timeOut	Use this element to set the ageing time of the ARP cache entries. Refer to The ARP cache time-out.	Default:00000d 02h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
proxyArp	Use this element to enable or disable the proxy ARP mechanism. Refer to What is proxy ARP?.	Default:enabled Range: enabled / disabled

What is the ARP cache?

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. This MAC address is not user configurable. The IP address of the LAN interface, on the other hand, is user configurable. This means that the user associates an IP address with the predefined MAC address. The MAC address - IP address pairs are kept in a table, called the ARP cache. Refer to telindus24xx/lanInterface/arpCache on page 489 for an example of such a table.

How does the ARP cache work?

Before the Telindus 2400 sends an IP packet on the LAN interface, it has to know the MAC address of the destination device. If the address is not present in the ARP cache table yet, the Telindus 2400 sends an ARP request on the Ethernet to learn the MAC address and associated IP address of the destination device. This address pair is then written in the ARP cache. Once the address pair is present, the Telindus 2400 can reference to this pair if it has to send an IP packet to the same device later on.

The ARP cache time-out

All the MAC address - IP address pairs from ARP requests and replies received on the LAN interface are kept in the ARP cache. However, if devices on the network are reconfigured then this MAC address - IP address relation may change. Therefore, the ARP cache entries are automatically removed from the cache after a fixed time-out. This time-out period can be set with the timeOut element.

What is proxy ARP?

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another device. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help devices on a subnet reach remote subnets without configuring routing or a default gateway.

The advantages and disadvantages of proxy ARP are listed below:

advantages	The main advantage of using proxy ARP is that it can be added to a single router on a network without disturbing the routing tables of the other routers on the network. Proxy ARP should be used on the network where IP hosts are not configured with default gateway or does not have any routing intelligence.
disadvantages	Hosts have no idea of the physical details of their network and assume it to be a flat network in which they can reach any destination simply by sending an ARP request. But using ARP for everything has disadvantages, some of which are listed below: • It increases the amount of ARP traffic on your segment. • Hosts need larger ARP tables to handle IP-to-MAC address mappings. • Security may be undermined. A device can claim to be another in order to intercept packets, an act called "spoofing". • It does not work for networks that do not use ARP for address resolution. • It does not generalise to all network topologies (for example, more than one router connecting two physical networks).

telindus24xx/lanInterface/bridging

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters of the LAN interface.

Refer to …

- 10 - Configuring bridging on page 223 for more information on bridging.
- 10.2.6 - Explaining the bridging structure on page 241 for a detailed description of the bridging structure.

telindus24xx/lanInterface/adapter

Default:autoDetect
Range: enumerated, see below

Use this attribute to set the Ethernet mode of the LAN interface.

The adapter attribute has the following values: autoDetect, 10Mb/halfDuplex, 10Mb/fullDuplex, 100Mb/halfDuplex, 100Mb/fullDuplex.

telindus24xx/lanInterface/vlan

Default:<empty>
Range: table, see below

Use this attribute to create and configure VLANs. Refer to 12.3 - Configuring VLANs on page 278 for an introduction and a step-by-step procedure.

As long as no VLANs are created in the vlan table, the LAN interface accepts both VLAN untagged and VLAN tagged frames. The VLAN *untagged* frames are bridged and/or routed (depending on the setting of the mode attribute). The VLAN *tagged* frames are bridged (in case the mode attribute is set to bridging or bridgingAndRouting, else they are discarded).

As soon as a VLAN is created in the vlan table, the LAN interface still accepts VLAN untagged frames but only accepts those VLAN tagged frames of which the VLAN ID corresponds with the VLAN ID that has been configured in the vlan table (refer to the configuration element vid on page 317). Other VLAN tagged frames are discarded.

The vlan table contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the VLAN. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate (down) the VLAN. Default:up Range: up / down
mode	Use this element to determine whether, for the corresponding VLAN, the packets are treated by the routing process or the bridging process. Default:bridging Range: enumerated, see below The mode element has the following values: **Value** / **Description** bridging: All packets received on the VLAN are bridged. routing: All packets received on the VLAN are routed.
ip	Use this element to configure the IP related parameters of the VLAN. Default:- Range: structure, see below Refer to … • 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses. • 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.
bridging	Use this element to configure the bridging related parameters of the VLAN. Default:- Range: structure, see below Refer to … • 10 - Configuring bridging on page 223 for more information on bridging. • 10.2.6 - Explaining the bridging structure on page 241 for a detailed description of the bridging structure.

Element	Description
vlan	Use this element to configure the specific VLAN parameters. Default:- Range: structure, see below Refer to telindus24xx/lanInterface/vlan/vlan on page 317 for a detailed description of the vlan structure.

telindus24xx/lanInterface/vlan/vlan

Default:-
Range: structure, see below

Use this structure to configure the specific VLAN related parameters of a VLAN.

The atm structure contains the following elements:

Element	Description
vid	Use this element to set the VLAN ID. Default:1 Range: 0 … 4095
tagSignificance	This element is only relevant when you set the mode element to bridging. Default:global Range: local / global Use this element to determine whether the VLAN tag has a local or a global significance. The tagSignificance element has the following values:

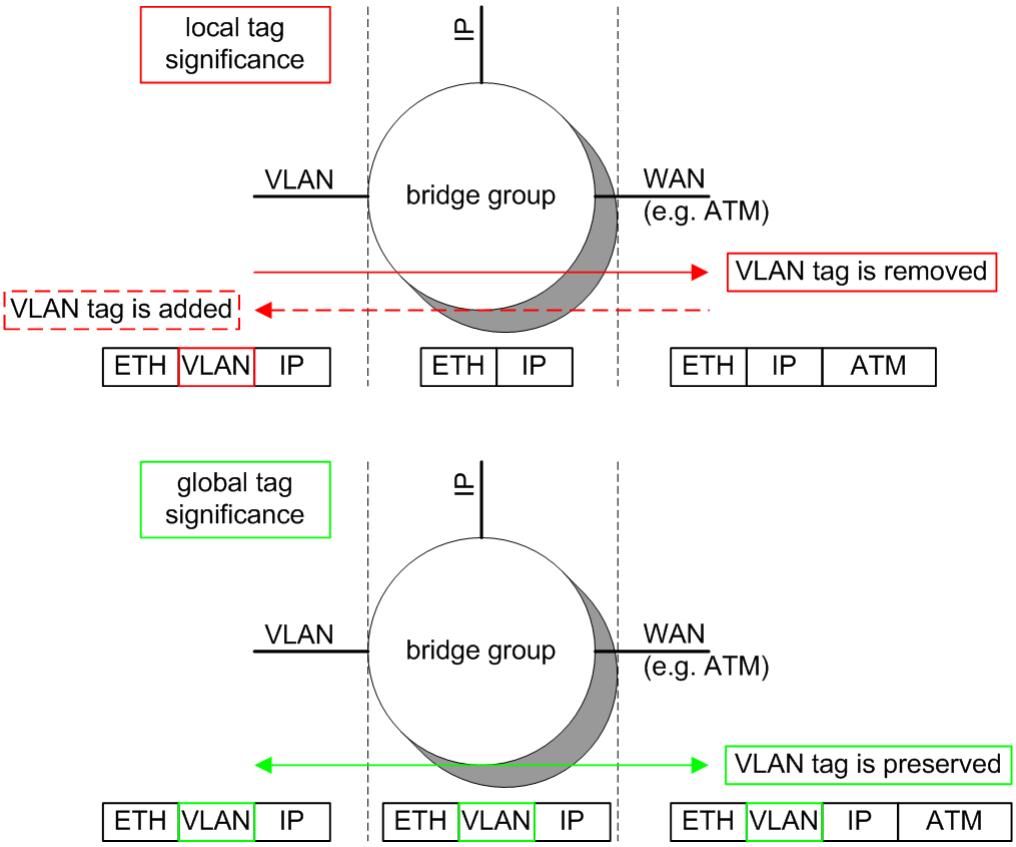
Value	Description
local	The VLAN tag only has a local significance, i.e. it is only present on the LAN interface side. This means that when the data is moved … • from the LAN interface to the bridge group, the VLAN tag is removed. • from the bridge group to the LAN interface, the VLAN tag is added. • Keep in mind that when the VLAN tag is removed, you not only discard the VLAN ID but also the user priority. • When you perform bridging between VLANs, then set the tagSignificance element to local. Else you get multiple VLAN tags in the Ethernet frames.
global	The VLAN tag has a global significance, i.e. it is both present on the LAN interface and the bridge group side. This means that when the data is moved from the LAN interface to the bridge group or vice versa, the VLAN tag is always preserved.

Refer to the figure Local or global VLAN tag significance on page 319.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>txCos</td><td>Use this element to set the default user priority (802.1P, also called COS) of the transmitted VLAN frames.
Default:0
Range: 0 … 7</td></tr>
<tr><td>changeTos</td><td>Use this element to enable or disable the COS to TOS and TOS to COS mapping.
Default:disabled
Range: enabled / disabled
If you set the changeTos attribute to disabled, then the elements cosTosMap and tosCosMap are ignored.</td></tr>
<tr><td>cosTosMap</td><td>Use this element to determine how the VLAN user priority (COS) maps onto the IP TOS byte value.
Default:-
Range: structure, see below
Note that the COS to TOS mapping only occurs in case …
• the mode element is set to routing and the changeTos element is set to enabled.
or
• the mode element is set to bridging, the changeTos element is set to enabled and the tagSignificance element is set to local.
The cosTosMap structure contains the following elements:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>p0 … p7</td><td>Use these elements to define which VLAN user priority (0 up to 7) maps onto which IP TOS byte value (0 up to 255).
Default:0
Range: 0 … 7</td></tr>
</table>
</td></tr>
<tr><td>tosCosMap</td><td>Use this element to determine how the IP TOS byte value maps onto the VLAN user priority (COS).
Default:-
Range: table, see below
Note that the COS to TOS mapping only occurs in case …
• the mode element is set to routing and the changeTos element is set to enabled.
or
• the mode element is set to bridging, the changeTos element is set to enabled and the tagSignificance element is set to local.
The tosCosMap table contains the following elements:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>startTos
endTos</td><td>Use these elements to set the TOS byte value range that has to be mapped.
Default:0
Range: 0 … 255</td></tr>
<tr><td>cos</td><td>Use this element to set the VLAN user priority (COS) value on which the specified TOS byte value range has to be mapped.
Default:0
Range: 0 … 7</td></tr>
</table>
</td></tr>
</table>

Local or global VLAN tag significance

The following figure shows how the tagSignificance element influences the VLAN tagging between the LAN interface and the bridge group:



telindus24xx/lanInterface/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask, alarmLevel, alarmContactHighMask and alarmContactLowMask and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the lanInterface object, refer to 16.4 - LAN interface alarms on page 651.

13.4 Cascading configuration attributes

This section describes the following configuration attributes:

• telindus24xx/lanInterface/atm/cascadeTable on page 321

telindus24xx/lanInterface/atm/cascadeTable

Default:<empty>
Range: table, see below

Use this attribute to cascade ATM switches. Refer to 11.3.3 - How to cascade ATM switches? on page 262 for a step-by-step procedure.

The cascadeTable contains the following elements:

Element	Description
name	Use this element to associate a name with the IP address you have to enter in the ip element. This name has to be used in the ATM switching table in case you want to cascade an ATM PVC from this ATM switch to another ATM switch. Default:<empty> Range: 0 … 24 characters
ip	Use this element to enter the LAN IP address of the ATM switch you want to cascade to. Default:0.0.0.0 Range: up to 255.255.255.255

13.5 4 port Ethernet interface configuration attributes

The configuration attributes of the 4 port Ethernet interface are the same as those of the LAN interface. Refer to 13.3 - LAN interface configuration attributes on page 312.

However, there is one exception: the configuration attribute adapter is present on the LAN interface, but not on the 4 port Ethernet interface. On the LAN interface you can use this attribute to select the Ethernet mode (auto, 10Mb/100Mb half/full duplex). On the 4 port Ethernet interface, the Ethernet mode is always detected automatically. It does this independently for each port (so it is possible that one port operates in 10Mb half duplex while another port operates in 100Mb full duplex).

13.6 6E1 interface configuration attributes

This section discusses the configuration attributes of the 6E1 interface. First it describes the configuration attributes of the interface as a whole, then of the separate E1 interfaces. Finally, it explains the ATM related attributes that can be configured per E1 interface.

The following gives an overview of this section:

- 13.6.1 - General 6E1 interface configuration attributes on page 324
- 13.6.2 - Specific E1 interface configuration attributes on page 328
- 13.6.3 - ATM configuration attributes on the E1 interface on page 331

This object only appears when the corresponding interface is inserted in the empty interface slot of the Telindus 2400. Refer to 2.6 - Connecting the Telindus 2400 on page 25.

13.6.1 General 6E1 interface configuration attributes

This section describes the following configuration attributes:

- telindus24xx/hexE1/ifClocking on page 325
- telindus24xx/hexE1/imaVersion on page 327
- telindus24xx/hexE1/imaDifferentialDelay on page 327

telindus24xx/hexE1/ifClocking

Default:external
Range: enumerated, see below

Use this attribute to set the clocking mode of the 6E1 interface.

The ifClocking attribute has the following values:

Value	Description
masterClock	The TIM interface clock is the same clock as the master clock (i.e. the clock that is used by the Telindus 2400 itself). Refer to telindus24xx/masterClock on page 309. If you set the ifClocking attribute to masterClock, then do not set the masterClock attribute to ifModule, since this is an illegal configuration.
external	If a valid signal is present on one of the E1 interfaces, then a clock signal is recovered from this signal and used as TIM interface clock. E1 interface 1 has the highest priority, E1 interface 6 has the lowest priority. So if a valid signal is present on all 6 E1 interfaces, then the TIM interface clock signal is recovered from E1 interface 1. Should the signal on E1 interface 1 drop, then the TIM interface clock signal is recovered from E1 interface 2. Etceteras.
e1_x	If a valid signal is present on the specified E1 interface (interface 1 up to 6), then a clock signal is recovered from this signal and used as TIM interface clock.
internal	The TIM interface clock is generated internally by the 6E1 interface.

telindus24xx/hexE1/imaVersion

Default:1.0
Range: enumerated, see below

Use this attribute to select the IMA version.

There are two IMA versions: 1.0 and 1.1. The IMA version 1.1 is a revision of the IMA version 1.0. The purpose of this revision is to introduce the IMA PICS proforma and a new version of the IMA MIBs as well as several minor corrections and clarifications to the content of IMA version 1.0. It is recognized that interoperability problems were generated by different interpretations of some IMA version 1.0 requirements. For this reason, the ATM Forum encourages the migration to IMA version 1.1. The IMA version 1.1 specification increments the OAM Label value used in the IMA OAM cells in order to differentiate version 1.1 from version 1.0 IMA units.

telindus24xx/hexE1/imaDifferentialDelay

Default:100ms
Range: enumerated, see below

Use this attribute to set the maximum amount of delay that is allowed between the different E1 links of an IMA group (i.e. the link differential delay tolerance).

The imaDifferentialDelay attribute has the following values: 50ms, 75ms, 100ms, 125ms, 150ms.

13.6.2 Specific E1 interface configuration attributes

This section describes the following configuration attributes:

- telindus24xx/hexE1/e1[E1_x]/name on page 329
- telindus24xx/hexE1/e1[E1_x]/coding on page 329
- telindus24xx/hexE1/e1[E1_x]/crc4Insertion on page 329
- telindus24xx/hexE1/e1[E1_x]/aisDetection on page 330
- telindus24xx/hexE1/e1[E1_x]/sqThreshold on page 330
- telindus24xx/hexE1/e1[E1_x]/sqTime on page 330
- telindus24xx/hexE1/e1[E1_x]/<alarmConfigurationAttributes> on page 330

telindus24xx/hexE1/e1[E1_x]/name

Default:<empty>
Range: 0 … 24 characters

Use this attribute to assign an administrative name to the E1 interface.

telindus24xx/hexE1/e1[E1_x]/coding

Default:hdb3
Range: hdb3 / ami

Use this attribute to determine which encoding mode is used on the E1 interface.

The coding attribute has the following values:

Value	Description
ami	Alternate Mark Inversion is selected. This is a bipolar code with no zero substitution.
hdb3	High Density Bipolar 3 is selected. This is a modified bipolar code. In case of HDB3 encoding, if more than three consecutive zeroes occur in the data they are replaced by a substitution word. This ensures a high pulse density. Therefore, data links using the HDB3 code can carry data patterns with a low 1 density. Most of the E1 applications use HDB3 encoding.

telindus24xx/hexE1/e1[E1_x]/crc4Insertion

Default:auto
Range: enumerated, see below

Use this attribute to determine whether the CRC-4 (Cyclic Redundancy Check) is inserted in the data or not. The CRC is used to check the data integrity on the E1 connection.

The crc4Insertion attribute has the following values:

Value	Description
auto	In auto mode, the CRC is inserted. Additionally … • if the CRC is present in the incoming data and … - if the CRC check is successful, then everything is OK. - if the CRC check fails, then the E-bit is set. However, the LFA alarm is not raised and the errored blocks are not counted (refer to the performance attribute errBlocks). • if the CRC is not present in the incoming data, then the E-bit is set. However, the LFA alarm is not raised.
enabled	The CRC is inserted. Additionally … • if the CRC is present in the incoming data and … - if the CRC check is successful, then everything is OK. - if the CRC check fails, then the LFA alarm is raised and the errored blocks count increases (refer to the performance attribute errBlocks). • if the CRC is not present in the incoming data, then the LFA alarm is raised.
disabled	The CRC is not inserted. Additionally, possible incoming CRCs are ignored.

telindus24xx/hexE1/e1[E1_x]/aisDetection

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the detection of the Alarm Indication Signal.

telindus24xx/hexE1/e1[E1_x]/sqThreshold

Default:10
Range: 0 … 65535

Use this attribute to set the signal quality threshold. This is the number of erroneous seconds for which a signal quality alarm is generated.

If the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime, then a signal quality (sq) alarm is generated.

For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated.

telindus24xx/hexE1/e1[E1_x]/sqTime

Default:00000d 00h 01m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the signal quality time. This is the period (in days, hours, minutes and seconds) during which the signal quality threshold is measured.

If the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime, then a signal quality (sq) alarm is generated.

For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated.

telindus24xx/hexE1/e1[E1_x]/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask, alarmLevel, alarmContactHighMask and alarmContactLowMask and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the e1[E1_x] object, refer to 16.6 - 6E1 interface alarms on page 653.

13.6.3 ATM configuration attributes on the E1 interface

This section describes the following configuration attributes:

• telindus24xx/hexE1/e1[E1_x]/atm/atmConfig on page 332

telindus24xx/hexE1/e1[E1_x]/atm/atmConfig

Default:-
Range: structure, see below

Use this attribute to configure some ATM related parameters for each E1 interface specifically.

The atmConfig structure contains the following elements:

Element	Description
scrambling	Use this element to enable or disable scrambling. Default:enabled Range: enabled / disabled Scrambling is designed to randomise the pattern of 1s and 0s carried in ATM cells or the physical layer frame. Randomising the digital bits can prevent continuous, non-variable bit patterns, in other words long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.
coset	Use this element to enable or disable coset polynomial algorithm. Default:enabled Range: enabled / disabled The coset polynomial algorithm is used to do header error check calculations.

Other devices that offer ATM encapsulation may allow you to configure the idle cell format. On the Telindus 2400 you can not configure this. The idle cell format is always ITU.

13.7 E3/T3 interface configuration attributes

This section discusses the configuration attributes of the E3/T3 interface. First it describes the specific E3/T3 interface configuration attributes. Then, it explains the ATM related attributes that can be configured on the E3/T3 interface.

The following gives an overview of this section:

- 13.7.1 - Specific E3/T3 interface configuration attributes on page 334
- 13.7.2 - ATM configuration attributes on the E3/T3 interface on page 337

This object only appears when the corresponding interface is inserted in the empty interface slot of the Telindus 2400. Refer to 2.6 - Connecting the Telindus 2400 on page 25.

13.7.1 Specific E3/T3 interface configuration attributes

This section describes the following configuration attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/ifClocking on page 335
- telindus24xx/e3T3/e3T3[E3T3_x]/aisDetection on page 335
- telindus24xx/e3T3/e3T3[E3T3_x]/sqThreshold on page 335
- telindus24xx/e3T3/e3T3[E3T3_x]/sqTime on page 335
- telindus24xx/e3T3/e3T3[E3T3_x]/<alarmConfigurationAttributes> on page 336

telindus24xx/e3T3/e3T3[E3T3_x]/ifClocking

Default:external
Range: enumerated, see below

Use this attribute to set the clocking mode of the E3/T3 interface.

The ifClocking attribute has the following values:

Value	Description
masterClock	The TIM interface clock is the same clock as the master clock (i.e. the clock that is used by the Telindus 2400 itself). Refer to telindus24xx/masterClock on page 309.
	If you set the ifClocking attribute to masterClock, then do not set the masterClock attribute to ifModule, since this is an illegal configuration.
external	If a valid signal is present on the E3/T3 interface, then a clock signal is recovered from this signal and used as TIM interface clock.
internal	The TIM interface clock is generated internally.

telindus24xx/e3T3/e3T3[E3T3_x]/aisDetection

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the detection of the Alarm Indication Signal.

telindus24xx/e3T3/e3T3[E3T3_x]/sqThreshold

Default:10
Range: 0 … 65535

Use this attribute to set the signal quality threshold. This is the number of erroneous seconds for which a signal quality alarm is generated.

If the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime, then a signal quality (sq) alarm is generated.

For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated.

telindus24xx/e3T3/e3T3[E3T3_x]/sqTime

Default:00000d 00h 01m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the signal quality time. This is the period (in days, hours, minutes and seconds) during which the signal quality threshold is measured.

If the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime, then a signal quality (sq) alarm is generated.

For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated.

telindus24xx/e3T3/e3T3[E3T3_x]/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask, alarmLevel, alarmContactHighMask and alarmContactLowMask and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the e3T3[E3T3_x] object, refer to 16.7 - E3/T3 interface alarms on page 654.

13.7.2 ATM configuration attributes on the E3/T3 interface

This section describes the following configuration attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc on page 338
- telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp on page 348

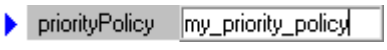
telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc

Default:<empty>
Range: table, see below

Use this attribute to set up ATM PVCs on the E3/T3 interface. So you have to add an entry to the pvc table for every ATM PVC that you want to create.

Note that you configure the complete ATM PVC, with all its parameters in this pvc table. This approach differs from how you have to configure ATM PVCs on the xDSL interfaces where you have to work with profiles.

The pvc table contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the PVC. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate (down) the PVC. Default:up Range: up / down
mode	Use this element to determine whether, for the corresponding PVC, the packets are treated by the routing process, the bridging process or the ATM switching process. Default:routing Range: enumerated, see below The mode element has the following values: **Value** / **Description** bridging: All packets received on the PVC are bridged. routing: All packets received on the PVC are routed. switching: All packets received on the PVC are switched.
priorityPolicy	Use this attribute to apply a priority policy on the PVC. Default:<empty> Range: 0 … 24 characters Do this by entering the index name of the priority policy you want to use. You can create the priority policy itself by adding a priorityPolicy[ ] object under the profiles/policy/priority object and by configuring the attributes in this object. **Example** If you created a priorityPolicy object with index name my_priority_policy (i.e. priorityPolicy[my_priority_policy]) and you want to apply this priority policy here, then enter the index name as value for the priorityPolicy attribute.  Refer to 9.7 - Configuring traffic and priority policy on the router on page 207 for more information on policies.
maxFifoQLen	Use this attribute to set the maximum length (number of packets) of the First In First Out queue. Default:200 Range: 1 … 4000 Refer to telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm on page 391 for more information on this queue.

Element	Description
ip	Use this element to configure the IP related parameters of the PVC. Default:- Range: structure, see below Refer to … • 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses. • 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.
bridging	Use this element to configure the bridging related parameters of the PVC in case the PVC is in bridging mode (i.e. in case the mode element is set to bridging). Default:- Range: structure, see below Refer to … • 10 - Configuring bridging on page 223 for more information on bridging. • 10.2.6 - Explaining the bridging structure on page 241 for a detailed description of the bridging structure.
atm	Use this element to configure the ATM related parameters of the PVC. Default:- Range: structure, see below Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm on page 340 for a detailed description of the atm structure.
ppp	Use this element to configure the PPP related parameters of the PVC in case you want to run PPP over ATM (i.e. in case the higherLayerProtocol element in the atm structure is set to ppp). Default:- Range: structure, see below Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/ppp on page 345 for a detailed description of the ppp structure.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm

Default:-
Range: structure, see below

Use this structure to configure the specific ATM related parameters of a PVC.

The atm structure contains the following elements:

Element	Description
vpi	Use this element to set the Virtual Path Identifier (VPI) of the ATM PVC. Default:0 Range: 0 … 7
vci	Use this element to set the Virtual Channel Identifier (VCI) of the ATM PVC. Default:32 Range: 32 … refer to specs You can configure multiple virtual channels per virtual path. Refer to What is VPI and VCI? on page 117.
qos	Use this element to select a QoS (Quality of Service). Default:<ubr> <Struct> Range: choice, see below Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/qos on page 342 for a detailed description of this element.
higherLayerProtocol	Use this attribute to select the protocol you want to run over ATM. Default:rfc2684 Range: enumerated, see below The higherLayerProtocol element has the following values:

Value	Description
rfc2684	Select this value in case you want to run bridged/routed Ethernet/IP over ATM (RFC 2684).
ppp	Select this value in case you want to run PPP over ATM (PPPoA, RFC 2364).

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>multiProtocolMech</td><td>Use this element to define how you want to encapsulate the higher layer protocol data in ATM.
Default:llcEncapsulation
Range: enumerated, see below

The multiProtocolMech element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>llcEncapsulation</td><td>Logical Link Control (LLC) encapsulation multiplexes multiple protocols over a single virtual connection. The protocol type of each protocol data unit (PDU) is identified by a prefixed IEEE 802.2 Logical Link Control (LLC) header.

In general, LLC encapsulation tends to require fewer VCs in a multi-protocol environment but has more fragmentation overhead.</td></tr>
<tr><td>vcMultiplexing</td><td>Virtual Circuit (VC) multiplexing uses one virtual connection to carry the PDUs of exactly one protocol type. When multiple protocols need to be transported, there is a separate VC for each.

VC multiplexing tends to reduce fragmentation overhead (e.g. an IPV4 datagram containing a TCP control packet with neither IP nor TCP options exactly fits into a single cell) but needs more VCs.</td></tr>
</table></td></tr>
<tr><td>inArpTimeOut</td><td>Use this element to set the time between the transmission of two consecutive Inverse ARP frames.
Default:00000d 00h 00m 30s
Range: 00000d 00h 00m 01s - 00000d 01h 00m 00s</td></tr>
<tr><td>oamF5Loopback</td><td>Use this element to configure the transmission of OAM F5 loop-back cells.
Default:-
Range: structure, see below

Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/oamF5Loopback on page 344 for a detailed description of this element.</td></tr>
</table>

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/qos

Default:<ubr> <Struct>
Range: choice, see below

Use this element to select a QoS (Quality of Service).

The first part of the qos element has the following values:

Value	Description
ubr	Select this value in case you want to select the Unspecified Bit Rate (UBR) service category. Then, using the second part of the qos element, you can configure the UBR related traffic parameters. The only UBR traffic parameter is the Peak Cell Rate (PCR). Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/qos/<ubr|vbrNrt> <Struct> on page 343 for more information on this parameter.

For more information on configuring ATM service categories, refer to …

- 7.1.5 - Configuring UBR on page 129

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/qos/<ubr> <Struct>

Default:-
Range: structure, see below

Use the elements in the structure located in the second part of the qos element to configure the traffic parameters related to the ATM service category that you selected using the first part of the qos attribute. Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/qos on page 342.

The structure located in the second part of the qos element can contain the following elements:

Element	Description
pcr	Use this element to set the Peak Cell Rate (PCR) of the ATM PVC. Default:0 Range: 0 … The pcr is expressed in kbps. Enter a multiple of 64 kbps as pcr value (e.g. 2048). The maximum value is the physical connection towards the ATM network.

For more information on how to use the traffic parameters in order to configure the ATM service categories, refer to …

- 7.1.5 - Configuring UBR on page 129

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/oamF5Loopback

Default:-
Range: structure, see below

Use the oamF5Loopback structure to configure the transmission of OAM F5 loop-back cells. Refer to What are OAM F5 loop-back cells? on page 122.

The oamF5Loopback structure contains the following elements:

Element	Description
operation	Use this element to enable or disable loop-back operation. Default:disabled Range: enabled / disabled The operation element has the following values: **Value** / **Description** disabled: Loop-back operation is disabled, i.e. the loop-back cells are not sent. This means that the ifOperStatus of the ATM PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the ATM PVC is configured (correctly) on the remote side. enabled: Loop-back operation is enabled, i.e. the Telindus 2400 sends loop-back cells at regular intervals. If consecutive cells are not returned by the remote side, then the ifOperStatus of the ATM PVC becomes down.
interval	Use this element to set the time interval between the sending of two consecutive loop-back cells. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
failsPermitted	Use this element to set the number of non-returned loop-back cells after which the Telindus 2400 declares the PVC down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If 10 consecutive loop-back cells are not returned by the remote side, then the Telindus 2400 declares the PVC down.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/ppp

Default:-
Range: structure, see below

Use this structure to configure the PPP related parameters of the PVC in case you want to run PPP over ATM (i.e. in case the higherLayerProtocol element in the atm structure is set to ppp).

The ppp structure contains the following elements:

Element	Description
linkMonitoring	Use this element to enable or disable and to fine-tune link monitoring. Default:- Range: structure, see below The linkMonitoring structure contains the following elements:

Element	Description
operation	Use this element to enable or disable link monitoring. Default:disabled Range: enabled / disabled
interval	Use this element to set the time interval between two consecutive echo requests. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
replyTimeOut	Use this element to set the time the Telindus 2400 waits for a reply on the echo request. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 00h 04m 15s If no reply has been received within this time-out, then the Telindus 2400 considers this as a failed echo request.
failsPermitted	Use this element to set the number of failed echo requests after which the Telindus 2400 declares the PPP link down. Default:4 Range: 1 ... 30 **Example** Suppose failsPermitted is set to 10. If on 10 consecutive echo requests no reply is given, then the Telindus 2400 declares the PPP link down and the PPP handshake is started again.

Refer to 7.2.5 - Configuring link monitoring on page 145 for more information on link monitoring.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>authentication</td><td>Use this element to enable or disable authentication on the PPP link.
Default:disabled
Range: enumerated, see below

The authentication element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Authentication is disabled.</td></tr>
<tr><td>pap</td><td>This side of the link requests a PAP authentication from the remote router.</td></tr>
<tr><td>chap</td><td>This side of the link requests a CHAP authentication from the remote router.</td></tr>
<tr><td>chapOrPap</td><td>This side of the link requests a CHAP or PAP authentication from the remote router.

If the remote router supports …
• only PAP, then PAP is used.
• only CHAP, then CHAP is used.
• both CHAP and PAP, then CHAP is used.</td></tr>
<tr><td>msChap</td><td>This side of the link requests an MS CHAP version 1 authentication from the remote router.</td></tr>
<tr><td>msChapV2</td><td>This side of the link requests an MS CHAP version 2 authentication from the remote router.</td></tr>
</table>

Refer to …
• 7.2.6 - Configuring PAP on page 146 for more information on PAP.
• 7.2.8 - Configuring CHAP on page 149 for more information on CHAP.</td></tr>
<tr><td>authenPeriod</td><td>Use this element to set the PPP authentication interval.
Default:00000d 00h 10m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Normally on an authenticated PPP link, authentication is not only performed at link set-up but also at regular intervals during the data transfer. You can set this interval using the authenPeriod attribute. If you set the authenPeriod attribute to 00000d 00h 00m 00s, then authentication is only performed at link set-up and not during the data transfer.

For more information on PPP authentication, refer to …
• 7.2.6 - Configuring PAP on page 146
• 7.2.8 - Configuring CHAP on page 149</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>compression</td><td>Use this element to enable or disable the compression of PPP encapsulated packets.
Default:disabled
Range: enumerated, see below

The compression element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>No PPP compression is done.</td></tr>
<tr><td>predictor1</td><td>PPP compression is done using the Predictor type 1 compression algorithm (RFC 1978). Using compression you can increase the throughput on PPP links.</td></tr>
</table>

Important remark

The PPP compression algorithm uses a lot of memory (64 KB for compression and 64 KB for decompression, per PPP session). Since it is possible to have multiple PPP sessions (when using ATM PVCs up to 31 simultaneous sessions are allowed, which can all be configured to use PPP compression), the memory can turn out to be insufficient. In this case …

• the compression is switched off on the interfaces that could not allocate enough memory,
• a message is dumped in the message table, containing the relevant interface and a warning that the router must be rebooted to reactivate compression on that specific interface.

It is also possible that, when looking at the statistics, enough memory seems to be available but that the allocation problem remains. This means that the memory is fragmented and no block as big as 64 KB is found.</td></tr>
</table>

telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp

Default:<empty>
Range: table, see below

Use this attribute to configure the transmission of OAM F4 loop-back cells. Refer to What are OAM F4 loop-back cells? on page 122. The entries in the vp table are used only in case an actual PVC is configured in the pvc table.

The vp table contains the following elements:

Element	Description
vpi	Use this element to enter the Virtual Path Identifier (VPI) of the Virtual Path for which you want to send the OAM F4 loop-back cells. Default:0 Range: 0 … 255
oamF4Loopback	Use this element to configure the transmission of OAM F4 loop-back cells. Default:- Range: structure, see below The elements contained in this structure are the same as those in the oamF5Loopback structure. For a detailed description of these elements refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc/atm/oamF5Loopback on page 344.

All entries in the vp configuration table are considered, even if for a certain VPI number no corresponding PVC has been configured. In the vp status and performance tables only the information about VPs that are configured in the vp configuration table is shown. However, the Telindus 2400 does respond to loop-back requests for VPs that are not configured in the vp configuration table but for which a PVC has been configured.

13.8 IMA group configuration attributes

This section describes the following configuration attributes:

- telindus24xx/bundle/imaGroup[ ]/members on page 350
- telindus24xx/bundle/imaGroup[ ]/minActiveLinks on page 350
- telindus24xx/bundle/imaGroup[ ]/pvc on page 350
- telindus24xx/bundle/imaGroup[ ]/vp on page 350
- telindus24xx/bundle/imaGroup[ ]/txFrameLength on page 351
- telindus24xx/bundle/imaGroup[ ]/rxFrameLength on page 351
- telindus24xx/bundle/imaGroup[ ]/traceMessages on page 351

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

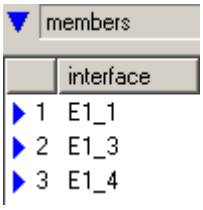
telindus24xx/bundle/imaGroup[ ]/members

Default:<empty>
Range: table, see below

Use this attribute to determine which E1 interfaces are member of the IMA group.

So you have to add an entry to the members table for every E1 interface that you want to include in the IMA group. Then type the index name of the E1 interface as value of the interface element.

For example, suppose you want to include E1 interface 1, 3 and 4 in the IMA group, then configure the members table as follows:



telindus24xx/bundle/imaGroup[ ]/minActiveLinks

Default:1
Range: 1 … 6

Use this attribute to determine what the minimum amount of E1 interfaces that have to be up before the IMA group may become active.

For example, suppose there are 6 E1 interfaces in the members table and you set the minActiveLinks attribute to 3, then the IMA group becomes active as soon as 3 E1 interfaces are up.

telindus24xx/bundle/imaGroup[ ]/pvc

Default:<empty>
Range: table, see below

Use this attribute to create ATM PVCs in the IMA group. So you have to add an entry to the pvc table for every ATM PVC that you want to create.

Note that you configure the complete ATM PVC, with all its parameters in this pvc table. This approach differs from how you have to configure ATM PVCs on the xDSL interfaces where you have to work with profiles.

Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc on page 338 for a detailed description of this attribute.

telindus24xx/bundle/imaGroup[ ]/vp

Default:<empty>
Range: table, see below

Use this attribute to configure the transmission of OAM F4 loop-back cells. Refer to What are OAM F4 loop-back cells? on page 122. The entries in the vp table are used only in case an actual PVC is configured in the pvc table.

Refer to telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp on page 348 for a detailed description of this attribute.

telindus24xx/bundle/imaGroup[ ]/txFrameLength

Default:128
Range: enumerated, see below

Use this attribute to set the IMA frame length, in cells, of the transmitter.

The txFrameLength attribute has the following values: 32, 64, 128, 256.

telindus24xx/bundle/imaGroup[ ]/rxFrameLength

Default:128
Range: enumerated, see below

Use this attribute to set the IMA frame length, in cells, of the receiver.

The rxFrameLength attribute has the following values: 32, 64, 128, 256.

telindus24xx/bundle/imaGroup[ ]/traceMessages

Default:disabled
Range: enumerated, see below

Use this attribute to enable or disable the sending of trace messages. These messages can be used for troubleshooting (debug) purposes.

The traceMessages attribute has the following values: disabled, icp, icp+events.

13.9 xDSL interface configuration attributes

This section describes the following configuration attributes:

- telindus24xx/dslInterfaces/ifClocking on page 353
- telindus24xx/dslInterfaces/interface[dsl_x]/lineConfiguration on page 353
- telindus24xx/dslInterfaces/interface[dsl_x]/<alarmConfigurationAttributes> on page 353

telindus24xx/dslInterfaces/ifClocking

Default:internal
Range: enumerated, see below

Use this attribute to set the clocking mode of the xDSL interface.

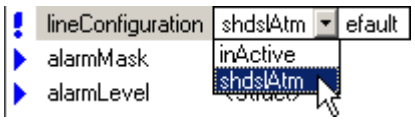
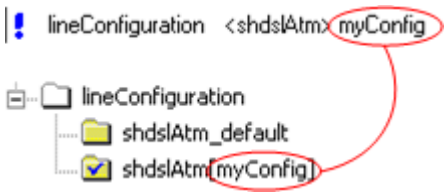
The ifClocking attribute has the following values:

Value	Description
masterClock	The xDSL interface clock is the same clock as the master clock (i.e. the clock that is used by the Telindus 2400 itself). Refer to telindus24xx/masterClock on page 309.
internal	The xDSL interface clock is generated internally.

telindus24xx/dslInterfaces/interface[dsl_x]/lineConfiguration

Default:inActive
Range: choice, see below

Use this attribute to apply a line configuration profile on the xDSL line. Do this as follows:

Step	Action
1	First select the type of configuration you want to apply. Do this by using the first part of the value field. If you want … • that the xDSL line is not active, then select inActive. • to apply an xDSL ATM configuration profile, then select xdslAtm (where xdsl can be shdsl or adsl). 
2	Then type the name of the line configuration profile you want to apply. Do this in the second part of the value field. If you want to apply … • a default line configuration profile, then type the string “default”. • a custom line configuration profile, then type the index name of the custom configuration object you previously added. E.g. type the string “myConfig” if the custom configuration object that you added is called configurations/xdslAtm[myConfig]. 

Refer to 5.2.5 - How to apply the line configuration profile? on page 82 for more information.

telindus24xx/dslInterfaces/interface[dsl_x]/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask and alarmLevel and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the interface[dsl_x] object, refer to 16.8.1 - General xDSL interface alarms on page 656.

13.10 Profile configuration attributes

This section discusses the configuration attributes of the different profiles that you can set up on the Telindus 2400. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.

The following gives an overview of this section:

- 13.10.1 - SHDSL profile configuration attributes on page 355
- 13.10.2 - ADSL profile configuration attributes on page 362
- 13.10.3 - ATM PVC profile configuration attributes on page 369
- 13.10.4 - Forwarding profile configuration attributes on page 378
- 13.10.5 - IP Traffic policy configuration attributes on page 380
- 13.10.6 - Bridging traffic policy configuration attributes on page 388
- 13.10.7 - Priority policy configuration attributes on page 390
- 13.10.8 - Line configuration profile configuration attributes on page 395

13.10.1 SHDSL profile configuration attributes

This section discusses the configuration attributes of the SHDSL profile. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.

This section describes the following configuration attributes:

- telindus24xx/profiles/xdsl/shdsl_default/region on page 356
- telindus24xx/profiles/xdsl/shdsl_default/mode on page 356
- telindus24xx/profiles/xdsl/shdsl_default/minSpeed on page 357
- telindus24xx/profiles/xdsl/shdsl_default/maxSpeed on page 357
- telindus24xx/profiles/xdsl/shdsl_default/minSpeed2P on page 357
- telindus24xx/profiles/xdsl/shdsl_default/maxSpeed2P on page 357
- telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds on page 358
- telindus24xx/profiles/xdsl/shdsl_default/retrain on page 359
- telindus24xx/profiles/xdsl/shdsl_default/management on page 360
- telindus24xx/profiles/xdsl/shdsl_default/<alarmConfigurationAttributes> on page 361

telindus24xx/profiles/xdsl/shdsl_default/region

Default:auto
Range: enumerated, see below

Use this attribute to select an SHDSL standard.

The region attribute has the following values:

Value	Description
annexA	The North-American SHDSL standard is used.
annexB	The European SHDSL standard is used.
auto	The Telindus 2400 itself determines which standard it has to use.

telindus24xx/profiles/xdsl/shdsl_default/mode

Default:dualPair
Range: singlePair / dualPair

Use this attribute to select between single pair or dual pair operation. When you change the mode attribute, then make sure that you use the correct speed attributes to set the speed:

If the mode attribute is set to …	then configure the speed using the attributes …
singlePair,	minSpeed and maxSpeed.
dualPair,	minSpeed2P and maxSpeed2P.

Refer to 6.3.3 - Creating a dual pair SHDSL line on page 100 for more information.

telindus24xx/profiles/xdsl/shdsl_default/minSpeed

Default:64kbps
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/shdsl_default/mode attribute is set to singlePair.

Use this attribute to set the lowest line speed the Telindus 2400 may select. The minSpeed attribute has the following values: 64kbps up to 2304kbps in steps of 64kbps.

Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information.

telindus24xx/profiles/xdsl/shdsl_default/maxSpeed

Default:2304kbps
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/shdsl_default/mode attribute is set to singlePair.

Use this attribute to set the highest line speed the Telindus 2400 may select. The maxSpeed attribute has the following values: 64kbps up to 2304kbps in steps of 64kbps.

Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information.

telindus24xx/profiles/xdsl/shdsl_default/minSpeed2P

Default:128kbps
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/shdsl_default/mode attribute is set to dualPair.

Use this attribute to set the lowest line speed the Telindus 2400 may select. The minSpeed2P attribute has the following values: 128kbps up to 4608kbps in steps of 128kbps.

Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information.

telindus24xx/profiles/xdsl/shdsl_default/maxSpeed2P

Default:2304kbps
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/shdsl_default/mode attribute is set to dualPair.

Use this attribute to set the highest line speed the Telindus 2400 may select. The maxSpeed2P attribute has the following values: 128kbps up to 4608kbps in steps of 128kbps.

Refer to 6.3.2 - Selecting an SHDSL line speed (range) on page 99 for more information.

telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds

Default:-
Range: structure, see below

Use this attribute to set the alarm threshold values of the most important line parameters. If this predefined threshold value is exceeded, then a corresponding alarm is generated.

The linkAlarmThresholds structure contains the following elements:

Element	Description
lineAttenuationOn	Use this element to set the alarm threshold value of the line attenuation in dB. If the line attenuation … Default:0.0 Range: 0.0 … 63.5 • exceeds this value during at least 10 seconds, then the lineAttenuation alarm is raised. • drops below this value during at least 10 seconds, then the lineAttenuation alarm is cleared.
noiseMarginOn	Use this element to set the alarm threshold value of the noise margin in dB. If the noise margin … Default:0.0 Range: 0.0 … 58.4 • drops below this value during at least 10 seconds, then the noiseMargin alarm is raised. • exceeds this value during at least 10 seconds, then the noiseMargin alarm is cleared.
errSecOn	Use this element to set the alarm threshold value of the erroneous seconds in days, hours, minutes and seconds. If the amount of erroneous seconds … Default:00000d 00h 00m 36s Range: 00000d 00h 00m 00s - 00000d 18h 12m 15s • exceeds this value within a 15 minutes period[1], then the errSecExceeded alarm is raised. • drops below this value within a 15 minutes period, then the errSecExceeded alarm is cleared.
sevErrSecOn	Use this element to set the alarm threshold value of the severely erroneous seconds in days, hours, minutes and seconds. If the amount of severely erroneous seconds … Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 18h 12m 15s • exceeds this value within a 15 minutes period[1], then the sevErrSecExceeded alarm is raised. • drops below this value within a 15 minutes period, then the sevErrSecExceeded alarm is cleared.

1. The 15 minutes periods run synchronous with the 15 minutes periods of the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line performance attribute.
   Because alarms are raised or cleared within 15 minutes periods, there is a delay in the alarm status. For example, suppose that in the first minute of a 15 minutes period the errSecOn value is exceeded, then the errSecExceeded alarm is raised. The alarm stays on for the remainder of the 15 minutes period. The alarm is only cleared if also in the next 15 minutes period the errSecOn value is not exceeded.

telindus24xx/profiles/xdsl/shdsl_default/retrain

Default:-
Range: structure, see below

Use this attribute to determine when the Telindus 2400 should retrain.

The retrain criteria

The following criteria determine when to retrain:

Criterion	Description
no SHDSL frame synchronisation	When the Telindus 2400 cannot synchronise on the SHDSL framing, it retrains.
SHDSL frame CRC error threshold exceeded	SHDSL framing sends 166 blocks per second over the line, independently of the speed. Each block has a CRC check. When a certain percentage of frames has a CRC error, the Telindus 2400 retrains.
noise margin too low	When the noise margin becomes too low during a certain period of time, the Telindus 2400 retrains.
layer 2 protocol not yet up	When you connect the Telindus 2400 with a remote SHDSL device, the Telindus 2400 trains and establishes a layer 1 link with the remote SHDSL device. Then the Telindus 2400 tries to establish a layer 2 link (e.g. PPP, FR, ATM). If the layer 2 handshake does not succeed within 1 minute, then the Telindus 2400 retrains and the whole process restarts. Also the following message is dumped in the message table: `Retrain due to framer-out-of-sync`. However, once the layer 2 handshake succeeds (layer 2 is up), then a drop of the layer 2 link will not cause a retrain.

Configuring the retrain criteria

The retrain structure contains the following elements:

Element	Description
enabled	Use this attribute to enable (yes) or disable (no) retraining. So when selecting no, the Telindus 2400 will never retrain (even not when the line is disconnected). In that case, the line just goes down (ifOperstatus = down). Default:yes Range: yes / no
errorPersistence-Time	Use this element to set the period, in seconds, during which each retrain criterion is measured. If within this period the predefined criterion value is equalled or exceeded, the Telindus 2400 retrains. Default:10 Range: 1 … 30
errorThreshold	Use this element to set the amount of CRC errors, in promille, at which the Telindus 2400 should retrain. If the amount of CRC errors exceeds this value, then the Telindus 2400 retrains. Default:10 Range: 1 … 1000 The erroneous SHDSL frames can be monitored using the performance attribute codeViolations.

Element	Description
noiseMarginThreshold	Use this element to set the noise margin, in dB, which has to be maintained. If the measured noise margin drops below this value, then the Telindus 2400 retrains. It will retrain at a lower speed (because of the deteriorated line conditions). Default:1dB Range: enumerated, see below The noiseMarginThreshold element has the following values: disabled, 1dB, 2dB, 3dB, 4dB, 5dB, 6dB. When you set the noiseMarginThreshold to disabled, the noise margin is ignored as retrain criterion.

telindus24xx/profiles/xdsl/shdsl_default/management

Default:o10-PathManagement
Range: enumerated, see below

Use this attribute to determine whether and which management data is forwarded over the SHDSL line.

The management attribute has the following possible values:

Value	Description
transparent	No management data is forwarded over the SHDSL line. The data is passed transparently over the line.
o10Management	This forwards the proprietary Telindus O10 protocol over the SHDSL line. This allows you to manage the remote SHDSL device (and possibly other Telindus devices connected to the SHDSL device).
pathManagement	This forwards path management information over the SHDSL line. This allows you to manage complete paths instead of managing individual devices (i.e. elements). Refer to the TMA Path Management manual (PDF) for more information.
o10-PathManagement	This forwards both the proprietary Telindus O10 protocol as the path management information over the SHDSL line.

telindus24xx/profiles/xdsl/shdsl_default/<alarmConfigurationAttributes>

Use the alarm related configuration attributes to configure the alarm behaviour of …

- the line object (use lineAlarmMask, lineAlarmLevel, lineAlarmContactHighMask and lineAlarmContactLowMask).
- the linePair[ ] object (use linePairAlarmMask, linePairAlarmLevel, linePairAlarmContactHighMask and linePairAlarmContactLowMask).
- the repeater object (use repeaterAlarmMask, repeaterAlarmLevel, repeaterLinePairAlarmMask and repeaterLinePairAlarmLevel). This is only relevant for the Telindus 2400 SHDSL models (2421, 2422, 2423).
- the end object (use endAlarmMask, endAlarmLevel, endLinePairAlarmMask and endLinePairAlarmLevel).

For more information on …

- the alarm configuration attributes and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the line object, refer to 16.8.2 - xDSL line alarms on page 657.
- the alarms of the linePair object, refer to 16.8.3 - xDSL line pair alarms on page 658.
- the alarms of the repeater object, refer to 16.8.4 - xDSL repeater and end alarms on page 660.
- the alarms of the end object, refer to 16.8.4 - xDSL repeater and end alarms on page 660.

13.10.2 ADSL profile configuration attributes

This section discusses the configuration attributes of the ADSL profile. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.

This section describes the following configuration attributes:

- telindus24xx/profiles/xdsl/adsl_default/standard on page 363
- telindus24xx/profiles/xdsl/adsl_default/usMinSpeed on page 364
- telindus24xx/profiles/xdsl/adsl_default/usMaxSpeed on page 364
- telindus24xx/profiles/xdsl/adsl_default/dsMinSpeed on page 364
- telindus24xx/profiles/xdsl/adsl_default/dsMaxSpeed on page 364
- telindus24xx/profiles/xdsl/adsl_default/retrain on page 364
- telindus24xx/profiles/xdsl/adsl_default/latency on page 365
- telindus24xx/profiles/xdsl/adsl_default/usInterleaveDelay on page 366
- telindus24xx/profiles/xdsl/adsl_default/dsInterleaveDelay on page 366
- telindus24xx/profiles/xdsl/adsl_default/usCorrectionTime on page 366
- telindus24xx/profiles/xdsl/adsl_default/dsCorrectionTime on page 366
- telindus24xx/profiles/xdsl/adsl_default/linkAlarmThresholds on page 367
- telindus24xx/profiles/xdsl/adsl_default/<alarmConfigurationAttributes> on page 368

telindus24xx/profiles/xdsl/adsl_default/standard

Default:multiMode
Range: enumerated, see below

Use this attribute to select an ADSL standard.

The standard attribute has the following values:

Value	Description
dmt	The ITU-T G.dmt or G992.1 standard is used. This is based on the ANSI T1.413 Issue 2 standard plus an extra handshaking protocol. It is capable of transmission speeds of up to 8 Mbps downstream and 864 Kbps upstream. **What is DMT?** The basic idea of DMT is to split the available bandwidth into a large number of subchannels. DMT is able to allocate data so that the throughput of every single subchannel is maximized. If some subchannel can not carry any data, it can be turned off and the use of available bandwidth is optimised.
lite	The ITU-T G.lite or G992.2 standard is used. This is a kind of stripped down ANSI T1.413 Issue 2 standard plus an extra handshaking protocol. It is capable of transmission speeds of up to 1.5 Mbps downstream and 512 Kbps upstream.
multiMode	The Telindus 2400 itself determines which standard it has to use. It chooses between DMT, Lite and T1.413. **Remark** Note that using the standard attribute you can not explicitly select T1.413 as ADSL standard. However, when setting the standard attribute to multiMode, it is possible that the ANSI T1.413 Issue 2 standard is selected as ADSL standard. You can check this by looking at the status attribute standard (refer to telindus24xx/dslInterfaces/interface[dsl_y]/line/standard on page 530). The ANSI T1.413 Issue 2 outlines the technical specifications of Discrete Multi-Tone (DMT). It is capable of transmission speeds of up to 8064 Kbps downstream and 1024 Kbps upstream.

What is the ADSL Annex?

The ADSL Annexes specify the following:

ADSL Annex	Description
Annex A	Specifies operation above the POTS band.
Annex B	Specifies operation above the ISDN band.

telindus24xx/profiles/xdsl/adsl_default/usMinSpeed

Default:32
Range: 32 ... 1536

Use this attribute to set the lowest upstream line speed the Telindus 2400 may select. The usMinSpeed attribute has the following values: 32 kbps up to 1536 kbps in steps of 32 kbps.

Refer to 6.4.2 - Selecting an ADSL line speed (range) on page 106 for more information.

telindus24xx/profiles/xdsl/adsl_default/usMaxSpeed

Default:1024
Range: 32 ... 1536

Use this attribute to set the highest upstream line speed the Telindus 2400 may select. The usMaxSpeed attribute has the following values: 32 kbps up to 1536 kbps in steps of 32 kbps.

Refer to 6.4.2 - Selecting an ADSL line speed (range) on page 106 for more information.

telindus24xx/profiles/xdsl/adsl_default/dsMinSpeed

Default:32
Range: 32 ... 12064

Use this attribute to set the lowest downstream line speed the Telindus 2400 may select. The dsMinSpeed attribute has the following values: 32 kbps up to 12064 kbps in steps of 32 kbps.

Refer to 6.4.2 - Selecting an ADSL line speed (range) on page 106 for more information.

telindus24xx/profiles/xdsl/adsl_default/dsMaxSpeed

Default:8064
Range: 32 ... 12064

Use this attribute to set the highest downstream line speed the Telindus 2400 may select. The dsMaxSpeed attribute has the following values: 32 kbps up to 12064 kbps in steps of 32 kbps.

Refer to 6.4.2 - Selecting an ADSL line speed (range) on page 106 for more information.

telindus24xx/profiles/xdsl/adsl_default/retrain

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable retraining of the ADSL line.

If the retrain attribute is set to enabled, then the Telindus 2400 automatically monitors the following statistics and attempts a full retrain when the following conditions occur:

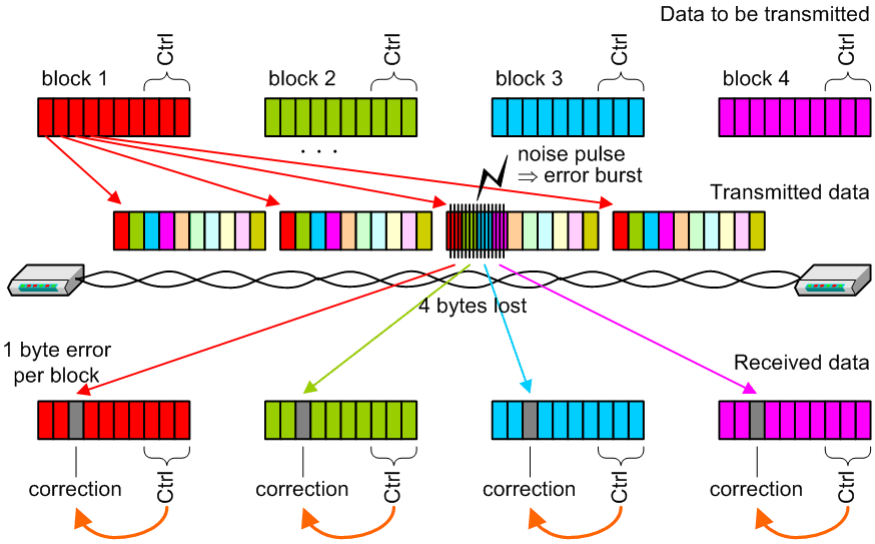
- One or more failures have occurred for 2.25 seconds or more.
- CRC error rate exceeds 40 per second for 10 consecutive seconds.

telindus24xx/profiles/xdsl/adsl_default/latency

Default:interleaved
Range: enumerated, see below

Use this attribute to configure the latency on the ADSL line.

The latency attribute has the following values:

Value	Description
interleaved	The data is spread out during ADSL transmission. This improves the ability to correct errors due to noise pulses and can thus make the connection more reliable. However, interleaving increases latency (delay). The amount of interleaving determines the amount of spread and hence the amount of latency.  You can configure the … • interleaving depth (i.e. the amount of interleaving), and hence the interleaving delay, using the attributes usInterleaveDelay and dsInterleaveDelay. Refer to telindus24xx/profiles/xdsl/adsl_default/usInterleaveDelay on page 366 and telindus24xx/profiles/xdsl/adsl_default/dsInterleaveDelay on page 366. • correction effort using the attributes usCorrectionTime and dsCorrectionTime. Refer to telindus24xx/profiles/xdsl/adsl_default/usCorrectionTime on page 366 and telindus24xx/profiles/xdsl/adsl_default/dsCorrectionTime on page 366.

Remark

On some ADSL modems you can set the latency to fast mode. In this mode no interleaving is done. This means that the connection has a lower latency but that it is more vulnerable to errors due to noise pulses. On the Telindus 2400 you can not select a fast mode, only interleaved mode (see above). However, the default values of the usInterleaveDelay, dsInterleaveDelay, usCorrectionTime and dsCorrectionTime attributes are chosen in such a way that a good trade-off between response time and robustness of the connection is obtained.

telindus24xx/profiles/xdsl/adsl_default/usInterleaveDelay

Default:2ms
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/adsl_default/latency attribute is set to interleaved.

Use this attribute to set the interleaving depth of the upstream data. The usInterleaveDelay attribute has the following values: 1ms, 2ms, 4ms, 8ms, 16ms, 32ms, 64ms.

The higher the interleave delay, the higher the interleaving depth (i.e. the amount of interleaving) and thus the higher the immunity to errors due to noise pulses.

telindus24xx/profiles/xdsl/adsl_default/dsInterleaveDelay

Default:4ms
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/adsl_default/latency attribute is set to interleaved.

Use this attribute to set the interleaving depth of the downstream data. The usInterleaveDelay attribute has the following values: 1ms, 2ms, 4ms, 8ms, 16ms, 32ms, 64ms.

The higher the interleave delay, the higher the interleaving depth (i.e. the amount of interleaving) and thus the higher the immunity to errors due to noise pulses.

telindus24xx/profiles/xdsl/adsl_default/usCorrectionTime

Default:500us
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/adsl_default/latency attribute is set to interleaved.

Use this attribute to set the correction time. This actually defines how large the error bursts may be that can still be corrected. The usCorrectionTime attribute has the following values: 125us, 250us, 500us, 1ms, 2ms, 4ms, disableRs.

Selecting disableRs disables the Reed Solomon (RS) error correction code. In this case no error correction is done. Error detection remains active.

telindus24xx/profiles/xdsl/adsl_default/dsCorrectionTime

Default:1ms
Range: enumerated, see below

This attribute is only relevant in case the telindus24xx/profiles/xdsl/adsl_default/latency attribute is set to interleaved.

Use this attribute to set the correction time. This actually defines how large the error bursts may be that can still be corrected. The dsCorrectionTime attribute has the following values: 125us, 250us, 500us, 1ms, 2ms, 4ms, disableRs.

Selecting disableRs disables the Reed Solomon (RS) error correction code. In this case no error correction is done. Error detection remains active.

telindus24xx/profiles/xdsl/adsl_default/linkAlarmThresholds

Default:-
Range: structure, see below

Use this attribute to set the alarm threshold values of the most important line parameters. If this predefined threshold value is exceeded, then a corresponding alarm is generated.

The linkAlarmThresholds structure contains the following elements:

Element	Description
lineAttenuationOn	Use this element to set the alarm threshold value of the line attenuation in dB. If the line attenuation … Default:0.0 Range: 0.0 … 63.5 • exceeds this value during at least 10 seconds, then the lineAttenuation alarm is raised. • drops below this value during at least 10 seconds, then the lineAttenuation alarm is cleared.
noiseMarginOn	Use this element to set the alarm threshold value of the noise margin in dB. If the noise margin … Default:0.0 Range: 0.0 … 58.4 • drops below this value during at least 10 seconds, then the noiseMargin alarm is raised. • exceeds this value during at least 10 seconds, then the noiseMargin alarm is cleared.
errSecOn	Use this element to set the alarm threshold value of the erroneous seconds in days, hours, minutes and seconds. If the amount of erroneous seconds … Default:00000d 00h 00m 36s Range: 00000d 00h 00m 00s - 00000d 18h 12m 15s • exceeds this value within a 15 minutes period[1], then the errSecExceeded alarm is raised. • drops below this value within a 15 minutes period, then the errSecExceeded alarm is cleared.
sevErrSecOn	Use this element to set the alarm threshold value of the severely erroneous seconds in days, hours, minutes and seconds. If the amount of severely erroneous seconds … Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 18h 12m 15s • exceeds this value within a 15 minutes period[1], then the sevErrSecExceeded alarm is raised. • drops below this value within a 15 minutes period, then the sevErrSecExceeded alarm is cleared.

1. The 15 minutes periods run synchronous with the 15 minutes periods of the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line performance attribute.
   Because alarms are raised or cleared within 15 minutes periods, there is a delay in the alarm status. For example, suppose that in the first minute of a 15 minutes period the errSecOn value is exceeded, then the errSecExceeded alarm is raised. The alarm stays on for the remainder of the 15 minutes period. The alarm is only cleared if also in the next 15 minutes period the errSecOn value is not exceeded.

telindus24xx/profiles/xdsl/adsl_default/<alarmConfigurationAttributes>

Use the alarm related configuration attributes to configure the alarm behaviour of …

- the line object (use lineAlarmMask, lineAlarmLevel, lineAlarmContactHighMask and lineAlarmContactLowMask).
- the linePair[ ] object (use linePairAlarmMask, linePairAlarmLevel, linePairAlarmContactHighMask and linePairAlarmContactLowMask).
- the end object (use endAlarmMask, endAlarmLevel, endLinePairAlarmMask and endLinePairAlarmLevel).

For more information on …

- the alarm configuration attributes and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the line object, refer to 16.8.2 - xDSL line alarms on page 657.
- the alarms of the linePair object, refer to 16.8.3 - xDSL line pair alarms on page 658.
- the alarms of the end object, refer to 16.8.4 - xDSL repeater and end alarms on page 660.

13.10.3 ATM PVC profile configuration attributes

This section discusses the configuration attributes of the ATM PVC profile. Refer to…

- 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.
- 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126 for more information on how to set up ATM PVCs using profiles.

This section describes the following configuration attributes:

- telindus24xx/profiles/atm/pvc_default/vpi on page 370
- telindus24xx/profiles/atm/pvc_default/vci on page 370
- telindus24xx/profiles/atm/pvc_default/qos on page 370
- telindus24xx/profiles/atm/pvc_default/higherLayerProtocol on page 372
- telindus24xx/profiles/atm/pvc_default/mode on page 376
- telindus24xx/profiles/atm/pvc_default/oamF5Loopback on page 377
- telindus24xx/profiles/atm/pvc_default/maxFifoQLen on page 377

telindus24xx/profiles/atm/pvc_default/vpi

Default:0
Range: 0 … 7

Use this attribute to set the Virtual Path Identifier (VPI) of the ATM PVC.

telindus24xx/profiles/atm/pvc_default/vci

Default:32
Range: 32 … refer to specs

Use this attribute to set the Virtual Channel Identifier (VCI) of the ATM PVC.

You can configure multiple virtual channels per virtual path. Refer to What is VPI and VCI? on page 117.

telindus24xx/profiles/atm/pvc_default/qos

Default:<ubr> <Struct>
Range: choice, see below

Use this attribute to select a QoS (Quality of Service).

The first part of the qos attribute has the following values:

Value	Description
ubr	Select this value in case you want to select the Unspecified Bit Rate (UBR) service category. Then, using the second part of the qos attribute, you can configure the UBR related traffic parameters. The only UBR traffic parameter is the Peak Cell Rate (PCR). Refer to telindus24xx/profiles/atm/pvc_default/qos/<ubr|vbrNrt> <Struct> on page 371 for more information on this parameter.

For more information on configuring ATM service categories, refer to …

- 7.1.5 - Configuring UBR on page 129

telindus24xx/profiles/atm/pvc_default/qos/<ubr> <Struct>

Default:-
Range: structure, see below

Use the elements in the structure located in the second part of the qos attribute to configure the traffic parameters related to the ATM service category that you selected using the first part of the qos attribute. Refer to telindus24xx/profiles/atm/pvc_default/qos on page 370.

The structure located in the second part of the qos attribute can contain the following elements:

Element	Description
pcr	Use this element to set the Peak Cell Rate (PCR) of the ATM PVC. Default:0 Range: 0 … The pcr is expressed in kbps. Enter a multiple of 64 kbps as pcr value (e.g. 2048). The maximum value is the physical connection towards the ATM network.

For more information on how to use the traffic parameters in order to configure the ATM service categories, refer to …

- 7.1.5 - Configuring UBR on page 129

telindus24xx/profiles/atm/pvc_default/higherLayerProtocol

Default:<rfc2684> llcEncapsulation
Range: choice, see below

Use this attribute to select the protocol you want to run over ATM.

The first part of the higherLayerProtocol attribute has the following values:

Value	Description
rfc2684	Select this value in case you want to run bridged/routed Ethernet/IP over ATM (RFC 2684). Then, using the second part of the higherLayerProtocol attribute, define how you want to encapsulate the data in ATM:

Value	Description
llcEncapsulation	Logical Link Control (LLC) encapsulation multiplexes multiple protocols over a single virtual connection. The protocol type of each protocol data unit (PDU) is identified by a prefixed IEEE 802.2 Logical Link Control (LLC) header. In general, LLC encapsulation tends to require fewer VCs in a multi-protocol environment but has more fragmentation overhead.
vcMultiplexing	Virtual Circuit (VC) multiplexing uses one virtual connection to carry the PDUs of exactly one protocol type. When multiple protocols need to be transported, there is a separate VC for each. VC multiplexing tends to reduce fragmentation overhead (e.g. an IPV4 datagram containing a TCP control packet with neither IP nor TCP options exactly fits into a single cell) but needs more VCs.

pppOverAtm	Select this value in case you want to run PPP over ATM (PPPoA, RFC 2364). Then, using the second part of the higherLayerProtocol attribute, configure the PPP related attributes. Refer to telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm> on page 373 for more information on these attributes.

telindus24xx/profiles/atm/pvc_default/higherLayerProtocol/<pppOverAtm>

Default:-
Range: structure, see below

If you set the first part of the higherLayerProtocol attribute to <pppOverAtm>, then use the structure in the second part of the higherLayerProtocol attribute to configure the PPP related attributes.

The <pppOverAtm> structure contains the following elements:

Element	Description
multiProtocolMech	Use this element to determine how the PPP protocol has to be encapsulated in ATM. Default:llcEncapsulation Range: enumerated, see below Possible values are: llcEncapuslation or vcMultiplexing. Refer to the explanation of the element rfc2684 on page 372 for more information on these values.
linkMonitoring	Use this element to enable or disable and to fine-tune link monitoring. Default:- Range: structure, see below The linkMonitoring structure contains the following elements:

Element	Description
operation	Use this element to enable or disable link monitoring. Default:disabled Range: enabled / disabled
interval	Use this element to set the time interval between two consecutive echo requests. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
replyTimeOut	Use this element to set the time the Telindus 2400 waits for a reply on the echo request. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 00s - 00000d 00h 04m 15s If no reply has been received within this time-out, then the Telindus 2400 considers this as a failed echo request.
failsPermitted	Use this element to set the number of failed echo requests after which the Telindus 2400 declares the PPP link down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If on 10 consecutive echo requests no reply is given, then the Telindus 2400 declares the PPP link down and the PPP handshake is started again.

Refer to 7.2.5 - Configuring link monitoring on page 145 for more information on link monitoring.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>authentication</td><td>Use this element to enable or disable authentication on the PPP link.
Default:disabled
Range: enumerated, see below

The authentication element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>Authentication is disabled.</td></tr>
<tr><td>pap</td><td>This side of the link requests a PAP authentication from the remote router.</td></tr>
<tr><td>chap</td><td>This side of the link requests a CHAP authentication from the remote router.</td></tr>
<tr><td>chapOrPap</td><td>This side of the link requests a CHAP or PAP authentication from the remote router.

If the remote router supports …
• only PAP, then PAP is used.
• only CHAP, then CHAP is used.
• both CHAP and PAP, then CHAP is used.</td></tr>
<tr><td>msChap</td><td>This side of the link requests an MS-CHAP authentication from the remote router.</td></tr>
<tr><td>msChapv2</td><td>This side of the link requests an MS-CHAP version 2 authentication from the remote router.</td></tr>
</table>

Refer to …
• 7.2.6 - Configuring PAP on page 146 for more information on PAP.
• 7.2.8 - Configuring CHAP on page 149 for more information on CHAP.</td></tr>
<tr><td>authenPeriod</td><td>Use this element to set the PPP authentication interval.
Default:00000d 00h 10m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Normally on an authenticated PPP link, authentication is not only performed at link set-up but also at regular intervals during the data transfer. You can set this interval using the authenPeriod attribute. If you set the authenPeriod attribute to 00000d 00h 00m 00s, then authentication is only performed at link set-up and not during the data transfer.

For more information on PPP authentication, refer to …
• 7.2.6 - Configuring PAP on page 146
• 7.2.8 - Configuring CHAP on page 149</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>compression</td><td>Use this element to enable or disable the compression of PPP encapsulated packets.
Default:disabled
Range: enumerated, see below

The compression element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>No PPP compression is done.</td></tr>
<tr><td>predictor1</td><td>PPP compression is done using the Predictor type 1 compression algorithm (RFC 1978). Using compression you can increase the throughput on PPP links.</td></tr>
</table>

Important remark

The PPP compression algorithm uses a lot of memory (64 KB for compression and 64 KB for decompression, per PPP session). Since it is possible to have multiple PPP sessions (when using ATM PVCs up to 31 simultaneous sessions are allowed, which can all be configured to use PPP compression), the memory can turn out to be insufficient. In this case …

• the compression is switched off on the interfaces that could not allocate enough memory,
• a message is dumped in the message table, containing the relevant interface and a warning that the router must be rebooted to reactivate compression on that specific interface.

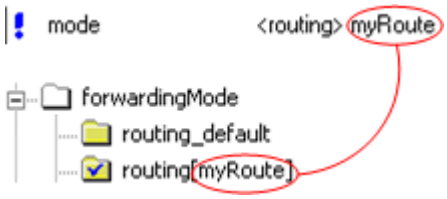
It is also possible that, when looking at the statistics, enough memory seems to be available but that the allocation problem remains. This means that the memory is fragmented and no block as big as 64 KB is found.</td></tr>
</table>

telindus24xx/profiles/atm/pvc_default/mode

Default:<routing> default
Range: choice, see below

Use this attribute to apply a forwarding profile on the ATM PVC profile. Do this as follows:

Step	Action
1	First select the type of forwarding you want to apply. Do this by using the first part of the value field. If you want to apply … • a routing forwarding profile, then select routing. • a bridging forwarding profile, then select bridging. • ATM switching, then select atmSwitching. Note that ATM switching does not have to be configured in a profile, but in the ATM switching table. So in that case, the second part of the higherLayerProtocol attribute has no function (see below).
2	Then type the name of the forwarding profile you want to apply. Do this in the second part of the value field. If you want to apply … • a default forwarding profile, then type the string “default”. • a custom forwarding profile, then type the index name of the custom forwarding object you previously added. E.g. type the string “myRoute” if the custom forwarding object that you added is called profiles/forwardingMode/routing[myRoute]. ATM switching does not have to be configured in a profile, but in the ATM switching table. So in case you set the first part of the higherLayerProtocol attribute to atmSwitching, then the second part of the higherLayerProtocol attribute has no function. Refer to 11.3 - Configuring ATM switching on page 256 for more information.



Refer to 5.2.2 - How to apply the forwarding profile? on page 77 for more information.

telindus24xx/profiles/atm/pvc_default/oamF5Loopback

Default:-
Range: structure, see below

Use the oamF5Loopback structure to configure the transmission of OAM F5 loop-back cells. Refer to What are OAM F5 loop-back cells? on page 122.

The oamF5Loopback structure contains the following elements:

Element	Description
operation	Use this element to enable or disable loop-back operation. Default:disabled Range: enabled / disabled The operation element has the following values: **Value** / **Description** disabled: Loop-back operation is disabled, i.e. the loop-back cells are not sent. This means that the ifOperStatus of the ATM PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the ATM PVC is configured (correctly) on the remote side. enabled: Loop-back operation is enabled, i.e. the Telindus 2400 sends loop-back cells at regular intervals. If consecutive cells are not returned by the remote side, then the ifOperStatus of the ATM PVC becomes down.
interval	Use this element to set the time interval between the sending of two consecutive loop-back cells. Default:00000d 00h 00m 10s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s
failsPermitted	Use this element to set the number of non-returned loop-back cells after which the Telindus 2400 declares the PVC down. Default:4 Range: 1 … 30 **Example** Suppose failsPermitted is set to 10. If 10 consecutive loop-back cells are not returned by the remote side, then the Telindus 2400 declares the PVC down.

telindus24xx/profiles/atm/pvc_default/maxFifoQLen

Default:200
Range: 1 … 4000

Use this attribute to set the maximum length (number of packets) of the First In First Out queue.

Refer to telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm on page 391 for more information on this queue.

13.10.4 Forwarding profile configuration attributes

This section discusses the configuration attributes of the forwarding profile. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.

This section describes the following configuration attributes:

- telindus24xx/profiles/forwardingMode/routing_default/ip on page 379
- telindus24xx/profiles/forwardingMode/bridging_default/bridging on page 379
- telindus24xx/profiles/forwardingMode/<routing|bridging_default>/priorityPolicy on page 379

telindus24xx/profiles/forwardingMode/routing_default/ip

Default:-
Range: structure, see below

This attribute is present in the routing forwarding profile.

Use this attribute to configure the IP related parameters of the forwarding profile. By doing so, you actually configure the IP related parameters of an ATM PVC and eventually of a DSL interface. This since the different profiles are applied as follows: forwarding profile → ATM PVC profile → line configuration profile → DSL interface.

Refer to …

- 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses.
- 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.

telindus24xx/profiles/forwardingMode/bridging_default/bridging

Default:-
Range: structure, see below

This attribute is present in the bridging forwarding profile.

Use this attribute to configure the bridging related parameters of the forwarding profile. By doing so, you actually configure the bridging related parameters of an ATM PVC and eventually of a DSL interface. This since the different profiles are applied as follows: forwarding profile → ATM PVC profile → line configuration profile → DSL interface.

Refer to …

- 10 - Configuring bridging on page 223 for more information on bridging.
- 10.2.6 - Explaining the bridging structure on page 241 for a detailed description of the bridging structure.

telindus24xx/profiles/forwardingMode/<routing|bridging_default>/priorityPolicy

Default:<empty>
Range: 0 … 24 characters

This attribute is present in the bridging and routing forwarding profile.

Use this attribute to apply a priority policy on this forwarding profile. By doing so, you actually apply a priority policy on an ATM PVC and eventually an a DSL interface. This since the different profiles are applied as follows: forwarding profile → ATM PVC profile → line configuration profile → DSL interface.

Apply the priority policy by entering the index name of the priority policy you want to use. You can create the priority policy itself by adding a priorityPolicy[ ] object under the profiles/policy/priority object and by configuring the attributes in this object.

Example

If you created a priorityPolicy object with index name my_priority_policy (i.e. priorityPolicy[my_priority_policy]) and you want to apply this priority policy here, then enter the index name as value for the priorityPolicy attribute.

Refer to 9.7 - Configuring traffic and priority policy on the router on page 207 for more information on policies.

13.10.5 IP Traffic policy configuration attributes

This section describes the following configuration attributes:

- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method on page 381
- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping on page 382
- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/dropLevels on page 385
- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping on page 387

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method

Default:trafficShaping
Range: enumerated, see below

Use this attribute to choose an IP traffic policy method. This IP traffic policy is then used to …

- determine, on traffic overload conditions, how and which queues are filled with the “excess” data. Refer to 9.7 - Configuring traffic and priority policy on the router on page 207.
- do policy based routing. Refer to 9.4 - Configuring policy based routing on page 176.
- filter data on an interface. Refer to 12.2 - Configuring an extended access list on page 271.

The method attribute has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>trafficShaping</td><td>The data is …
redirected to the queues based on the settings of the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping (queueing).
redirected to an interface or a gateway based on the settings of the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping (policy based routing).
filtered based on the settings of the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping (extended access list).</td></tr>
<tr><td>tosDiffServ</td><td>The data is redirected to the queues based on DiffServ (refer to RFC 2597) regarding class and drop precedence. Refer to What is AF PHB? on page 209.

This means that, depending on their DSCP field in the TOS byte, some packets are moved to other queues and/or dropped sooner than other packets in case the queue is full.

The highest 3 bits of the DSCP field are mapped as follows:<table><tr><th>Bit values …</th><th>are mapped to …</th></tr><tr><td>000 up to 100</td><td>queues 1 up to 5, respectively.</td></tr><tr><td>101 and higher</td><td>the low delay queue.</td></tr></table>The next 2 bits of the DSCP field define the drop levels:<table><tr><th>Bit values …</th><th>correspond with …</th></tr><tr><td>00 and 01</td><td>dropLevel1</td></tr><tr><td>10</td><td>dropLevel2</td></tr><tr><td>11</td><td>dropLevel3</td></tr></table>Refer to the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/dropLevels for more information on drop levels.</td></tr>
<tr><td>tosMapped</td><td>The data is redirected to …
the queues based on the settings of the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping (queueing).
an interface or a gateway based on the settings of the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping (policy based routing).</td></tr>
</table>

telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/trafficShaping

Default:<empty>
Range: table, see below

The function of this attribute is threefold:

- **Traffic and priority policing**
  In case you have set the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data has to be redirected to which queue. If an overload condition occurs, then a packet is redirected to the specified queue when the criteria as specified in the trafficShaping table are met.
  Refer to 9.7 - Configuring traffic and priority policy on the router on page 207.
- **Policy based routing**
  In case you have set the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data has to be redirected to which interface or gateway. Packets are redirected to the specified interface or gateway when the criteria as specified in the trafficShaping table are met.
  Refer to 9.4 - Configuring policy based routing on page 176.
- **Extended access list**
  In case you have set the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method attribute to trafficShaping, then use the trafficShaping table to specify which data is forwarded. Packets are forwarded when the criteria as specified in the trafficShaping table are met. If more than one entry applies to the same packet, then the entry which has the narrowest filter range (when looking at the filter criteria from left to right) is chosen.
  Refer to 12.2 - Configuring an extended access list on page 271.

Important remark

If a traffic shaping table is applied on an interface, then it discards all traffic that does not match the entries in the table. This is independent whether the traffic shaping table is used as an access list, for priority policing or policy based routing.

The trafficShaping table contains the following elements:

Element	Description
sourceIpStart-Address	Use these elements to set the IP source address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
sourceIpEnd-Address	Packets that fall within the specified range are forwarded and queued if applicable.
destinationIpStart-Address	Use these elements to set the IP destination address as specified in the IP header. Default:0.0.0.0 Range: up to 255.255.255.255
destinationIpEnd-Address	Packets that fall within the specified range are forwarded and queued if applicable.
tosStartValue	Use these elements to set the TOS byte value. Default:any(start)/optional(end) Range: 0 … 256
tosEndValue	Packets that fall within the specified range are forwarded and queued if applicable.

Element	Description
ipProtocol	Use this element to set the protocol field from the IP header. Default:any Range: 0 … 255 Packets that have the specified protocol field are forwarded and queued if applicable. You can specify the protocol by typing the protocol number. For ease of use, some common protocols can be selected from a drop-down box: any (0), ICMP (1), IGMP (2), IPinIP (4), TCP (6), EGP (8), IGP (9), UDP (17), RSVP (46), IGRP (88), OSPFIGP (89), TCPestablished (255).
sourcePortStart sourcePortEnd	Use these elements to set the source port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: any or optional (0), echo (7), discard (9), ftp-data (20), ftp (21), telnet (23), smtp (25), domain (53), www-http (80), pop3 (110), nntp (119), snmp (161), snmptrap (162), z39.50 (210), syslog (514), router (520), socks (1080), l2tp (1701), telindus (1728).
destinationPortStart destinationPortEnd	Use these elements to set the destination port as specified in the UDP / TCP headers. Default:any(start)/optional(end) Range: 0 … 65535 Packets that fall within the specified range are forwarded and queued if applicable. You can specify the port by typing the protocol number. For ease of use, some common port numbers can be selected from a drop-down box: see above.
newTosValue	Use this element to set the new TOS byte value. Default:unchanged Range: 0 … 256 When you select a new TOS byte value, then a packet that matches an entry in the trafficShaping table its TOS byte value is changed. Selecting unchanged, leaves the TOS byte value as it is.
priority	Use this element to set the destination queue for a packet matching an entry in the trafficShaping table. Default:queue1 Range: enumerated, see below In case an overload condition occurs, then a packet that matches an entry in the trafficShaping table is sent to the specified queue. The priority element has the following values: queue1, queue2, queue3, queue4, queue5, lowDelayQueue.
interface	Use this element to set the destination interface for a packet matching an entry in the trafficShaping table. This is policy based routing. Default:<empty> Range: 0 … 24 characters Type the name of the interface in the interface element, e.g. lan.
gateway	Use this element to set the gateway for a packet matching an entry in the trafficShaping table. This is policy based routing. Default:<opt> Range: up to 255.255.255.255

Start and end values

Except for the ipProtocol, newTosValue and priority elements, it is possible to specify ranges using the start and end values. There are two special cases:

- A start value is entered, but no end value ⇒ an exact match is needed for the start value.
- Neither a start nor an end value is entered ⇒ the field is not checked.

telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/dropLevels

Default:-
Range: table, see below

Use this attribute to define for each user configurable queue, how many packets may be queued before they are dropped.

The dropLevels table contains the following elements:

Element	Description
dropLevel1	Use this element to set the maximum length (drop level 1), in packets, of each user configurable queue. Default:100 Range: 1 … 3000 In case you set the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method to … • trafficShaping or tosMapped, then only this drop level is relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 00 and 01.
dropLevel2	Use this element to set the maximum length (drop level 2), in packets, of each user configurable queue. Default:100 Range: 1 … 3000 In case you set the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 10.
dropLevel3	Use this element to set the maximum length (drop level 3), in packets, of each user configurable queue. Default:100 Range: 1 … 3000 In case you set the attribute telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method to … • trafficShaping or tosMapped, then this drop level is not relevant. • tosDiffServ, then this drop level corresponds with the drop level bits value 11.

Examples

Suppose …

- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method is set to trafficShaping or tosMapped.
- for queue 1 you set maxLength1 = 1000, for queue 2 to 500, for queue 3 to 3000, for queue 4 to 1000 and for queue 5 to 200.

In this case, packets are dropped when the amount of packets in the queue exceeds the amount as specified with the maxLength1 element.

Suppose …

- telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method is set to tosDiffServ.
- for queue 1 you set maxLength1 = 100, maxLength2 = 200 and maxLength3 = 50.

In this case, the following applies:

Queue 1 contains … data packets.	**An incoming data packet with … is …**		
	drop level[1] 1	**drop level 2**	**drop level 3**
less than 50	accepted	accepted	accepted
more than 50, less than 100	accepted	accepted	dropped
more than 100, less than 200	dropped	accepted	dropped
more than 200	dropped	dropped	dropped

1. As defined in the TOS byte.

telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/tos2QueueMapping

Default:<empty>
Range: table, see below

The function of this attribute is twofold:

- **Traffic and priority policing**
  In case you have set the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method attribute to tosMapped, then use the tos2QueueMapping table to specify which data has to be redirected to which queue. If an overload condition occurs, then a packet is redirected to the specified queue when the criteria as specified in the tos2QueueMapping table are met.
  Refer to 9.7 - Configuring traffic and priority policy on the router on page 207 and 10.3 - Configuring traffic and priority policy on the bridge on page 245.
- **Policy based routing**
  In case you have set the telindus24xx/profiles/policy/traffic/ipTrafficPolicy[ ]/method attribute to tosMapped, then use the tos2QueueMapping table to specify which data has to be redirected to which interface or gateway. Packets are redirected to the specified interface or gateway when the criteria as specified in the tos2QueueMapping table are met.
  Refer to 9.4 - Configuring policy based routing on page 176.

The tos2QueueMapping table contains the following elements:

Element	Description
startTos endTos	Use these elements to set the TOS byte value. Packets that have a TOS byte value within the specified range are redirected to the targetQueue. Default:0 (start) / 255 (end) Range: 0 … 255
targetQueue	Use this element to set the destination queue. The targetQueue element has the following values: Queue1, Queue2, Queue3, Queue4, Queue5, lowDelayQueue. Default:Queue1 Range: enumerated, see below
interface	Use this element to set the destination interface for a packet matching an entry in the tos2QueueMapping table. This is policy based routing. Type the name of the interface in the interface element, e.g. lan. Default:<empty> Range: 0 … 24 characters
gateway	Use this element to set the gateway for a packet matching an entry in the tos2QueueMapping table. This is policy based routing. Default:<opt> Range: up to 255.255.255.255

13.10.6 Bridging traffic policy configuration attributes

This section describes the following configuration attributes:

- telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/vlanPriorityMap on page 389
- telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/dropLevels on page 389

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/vlanPriorityMap

Default:-
Range: structure, see below

Use this attribute to impose a bridging traffic policy on the bridged VLAN frames received by the Telindus 2400.

Each VLAN frame has a certain priority (this is specified in the 802.1P part of the 802.1Q header of the VLAN frame). In case a traffic overload condition occurs and in case you imposed this traffic policy on a certain interface, then the VLAN frames are sent to a queue. Using the vlanPriorityMap attribute, you can specify which VLAN frame is sent to which queue based on the priority of the VLAN frame.

The vlanPriorityMap structure contains the following elements:

Element	Description
priority0 … priority7	Use these elements to define which priority corresponds with which queue. The possible queues are: queue1 up to queue5 and lowDelayQueue. To empty these queues, specify a priority policy. Frames that are not tagged are all considered to have priority 0. Refer to 10.3 - Configuring traffic and priority policy on the bridge on page 245 for more information on traffic policy, priority policy and priority queuing.

telindus24xx/profiles/policy/traffic/bridgingTrafficPolicy[ ]/dropLevels

Default:-
Range: table, see below

Use this attribute to define for each user configurable queue, how many packets may be queued before they are dropped.

The dropLevels table contains the following element:

Element	Description	
dropLevel1	Use this element to set the maximum length, in packets, of each user configurable queue.	Default:100 Range: 1 … 3000

13.10.7 Priority policy configuration attributes

This section describes the following configuration attributes:

- telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm on page 391
- telindus24xx/profiles/policy/priority/priorityPolicy[ ]/countingPolicy on page 394
- telindus24xx/profiles/policy/priority/priorityPolicy[ ]/queueConfigurations on page 394
- telindus24xx/profiles/policy/priority/priorityPolicy[ ]/lowdelayQuotum on page 394

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm

Default:fifo
Range: enumerated, see below

Use this attribute to determine how and which queues are emptied.

The algorithm attribute has the following values:

Value	Description
fifo	This is a First In First Out queue. The data that enters the queue first, also leaves the queue first. This is the fastest but most superficial queuing mechanism. You can change the maximum length of the FIFIO queue on an interface using the configuration attribute maxFifoQLen.
roundRobin	This is a priority queuing mechanism. In this case, all user configurable queues containing data have an equal weight. In other words, if all the user configurable queues contain data, they are addressed in turns. The low delay has a higher priority, it is addressed between every user configurable queue. The system queue has absolute priority, it is emptied as soon as it contains data.

Queue	Priority
1 - 5 : user configurable queue	These queues are addressed in turns.
6 : low delay queue	This queue is addressed between every user configurable queue.
7 : system queue	This queue has absolute priority over all other queues. As soon as it contains data, it is emptied.

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>absolutePriority</td><td>This is a priority queuing mechanism. In this case, queues with a high priority have absolute priority over queues with a low priority. In other words, no lower priority queue is emptied as long as a higher priority queue contains data.

The priority of the queues runs parallel to the queue number. I.e. the user configurable queue number 1 has the lowest priority, whereas the system queue (number 7) has the highest priority.

<table>
<tr><th>Queue</th><th>Priority</th></tr>
<tr><td>1 - 5 : user configurable queue</td><td>Queue 1 has the lowest priority whereas queue 5 has the highest priority. A lower priority queue is only emptied in case no higher priority queue contains data.</td></tr>
<tr><td>6 : low delay queue</td><td>This queue is only emptied in case the system queue contains no data.</td></tr>
<tr><td>7 : system queue</td><td>This queue has absolute priority over all other queues. As soon as it contains data, it is emptied.</td></tr>
</table>

Note that there is a risk of starvation. This means that it is possible that the lower priority queues are never emptied because a higher priority queue continuously receives data.</td></tr>
<tr><td>weightedFair-Queueing</td><td>This is a priority queuing mechanism. In this case, the user configurable queues are addressed based on their weight. The low delay has a higher priority, it is addressed between every user configurable queue. The system queue has absolute priority, it is emptied as soon as it contains data.

<table>
<tr><th>Queue</th><th>Priority</th></tr>
<tr><td>1 - 5 : user configurable queue</td><td>These queues are addressed based on their weight. The weight can be configured in the telindus24xx/profiles/policy/priority/priorityPolicy[ ]/queueConfigurations attribute.</td></tr>
<tr><td>6 : low delay queue</td><td>This queue is addressed between every user configurable queue.</td></tr>
<tr><td>7 : system queue</td><td>This queue has absolute priority over all other queues. As soon as it contains data, it is emptied.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>lowDelayWeighted-FairQueueing</td><td>This is a priority queuing mechanism. It is a combination of absolute priority and weighted fair queueing. In this case, the user configurable queues are addressed based on their weight. The low delay queue has absolute priority over all user configurable queues and the system queue has absolute priority over all queues.
<table>
<tr><th>Queue</th><th>Priority</th></tr>
<tr><td>1 - 5 : user configurable queue</td><td>These queues are addressed based on their weight. The weight can be configured in the telindus24xx/profiles/policy/priority/priorityPolicy[ ]/queueConfigurations attribute.</td></tr>
<tr><td>6 : low delay queue</td><td>This queue has absolute priority over all user configurable queues. If the system queue does not contain data but the low delay queue and the user configurable queues do, then it is the low delay queue that is emptied.</td></tr>
<tr><td>7 : system queue</td><td>This queue has absolute priority over all other queues. As soon as it contains data, it is emptied.</td></tr>
</table>

In a network that carries both voice and data, the lowDelayWeightedFairQueueing algorithm is the most suited mechanism to get the voice over the network with a minimum delay. In this case, the voice has to be queued in the low delay queue.</td></tr>
</table>

telindus24xx/profiles/policy/priority/priorityPolicy[ ]/countingPolicy

Default:bytes
Range: enumerated, see below

Use this attribute to define whether the quotum of the queues is expressed in bytes or packets.

telindus24xx/profiles/policy/priority/priorityPolicy[ ]/queueConfigurations

Default:<empty>
Range: table, see below

Use this attribute to …

- set the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed.
- set the relative importance of the user configurable queues.

The queueConfigurations table contains the following elements:

Element	Description
quotum	Use this element to set the number of bytes/packets that is dequeued from the user configurable queue when the queue is addressed. Default:1500 Range: 1 … 25000 The unit of the quotum (bytes or packets) can be set with the telindus24xx/profiles/policy/priority/priorityPolicy[ ]/countingPolicy attribute.
weight	Use this element to set the relative importance of the user configurable queues. Default:1 Range: 1 … 10 The weight element is only relevant in case the telindus24xx/profiles/policy/priority/priorityPolicy[ ]/algorithm attribute is set to weightedFairQueueing. **Example** Suppose queue 1 has weight 2, queue 2 has weight 1 and both queues contain data. In that case the queues are emptied in the following order: queue 1 → queue 1 → queue 2 → queue 1 → queue 1 → queue 2 → etc.

Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for more information on queues.

telindus24xx/profiles/policy/priority/priorityPolicy[ ]/lowdelayQuotum

Default:1500
Range: 1 … 25000

Use this attribute to set the number of bytes/packets that is dequeued from the low delay queue when the queue is addressed. The unit of the quotum (bytes or packets) can be set with the telindus24xx/profiles/policy/priority/priorityPolicy[ ]/countingPolicy attribute.

Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for more information on queues.

13.10.8 Line configuration profile configuration attributes

This section discusses the configuration attributes of the line configuration profile. Refer to 5 - Configuring the Telindus 2400 - the concept of profiles on page 63 for more information on how to use profiles to configure the Telindus 2400.

This section describes the following configuration attributes:

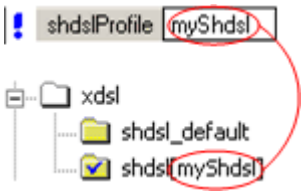
- telindus24xx/profiles/lineConfiguration/xdslAtm_default/xdslProfile on page 396
- telindus24xx/profiles/lineConfiguration/xdslAtm_default/pvc on page 396
- telindus24xx/profiles/lineConfiguration/xdslAtm_default/vp on page 397

telindus24xx/profiles/lineConfiguration/xdslAtm_default/xdslProfile

Default:default
Range: 0 … 24 characters

Use this attribute to apply an xDSL profile on the line configuration profile.

Do this by typing the name of the xDSL profile you want to apply as value of the shdslProfile attribute. If you want to apply …



- a default xDSL profile, then type the string “default”.
- a custom xDSL profile, then type the index name of the custom xDSL object you previously added. E.g. type the string “myXdsl” if the custom xDSL object that you added is called profiles/xdsl/profile[myXdsl].

Refer to 5.2.4 - How to apply the xDSL and ATM PVC profiles? on page 80 for more information.

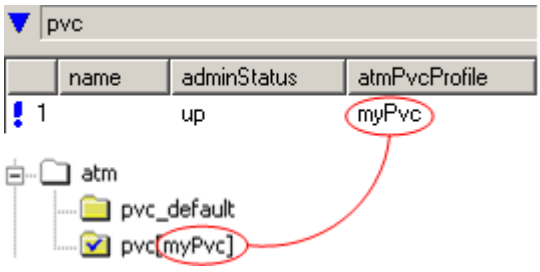
telindus24xx/profiles/lineConfiguration/xdslAtm_default/pvc

Default:<empty>
Range: table, see below

Use this attribute to determine which profile is applied on each ATM PVC. So you have to add an entry to the pvc table for every ATM PVC that you want to create (on a specific xDSL line). The actual configuration of the ATM PVCs (i.e. setting the VPI, VCI, PCR, etc.) has already been done in the ATM PVC profile.

The pvc table contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the ATM PVC. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate (down) the ATM PVC. Default:up Range: up / down
atmPvcProfile	Use this element to apply an ATM PVC profile on the ATM PVC. Default:default Range: 0 … 24 characters Do this by typing the name of the ATM PVC profile you want to apply as value of the atmPvcProfile element. If you want to apply … • a default ATM PVC profile, then type the string “default”. • a custom ATM PVC profile, then type the index name of the custom ATM PVC object you previously added. E.g. type the string “myPvc” if the custom ATM PVC object that you added is called profiles/atm/pvc[myPvc]. Refer to 5.2.4 - How to apply the xDSL and ATM PVC profiles? on page 80 for more information.



Refer to 7.1.4 - Configuring ATM PVCs - the ATM PVC profile on page 126 for more information on setting up ATM PVCs.

telindus24xx/profiles/lineConfiguration/xdslAtm_default/vp

Default:<empty>
Range: table, see below

Use this attribute to configure the transmission of OAM F4 loop-back cells. Refer to What are OAM F4 loop-back cells? on page 122. The entries in the vp table are used only in case an actual PVC is configured in the pvc table.

The vp table contains the following elements:

Element	Description
vpi	Use this element to enter the Virtual Path Identifier (VPI) of the Virtual Path for which you want to send the OAM F4 loop-back cells. Default:0 Range: 0 … 255
oamF4Loopback	Use this element to configure the transmission of OAM F4 loop-back cells. Default:- Range: structure, see below The elements contained in this structure are the same as those in the oamF5Loopback structure. For a detailed description of these elements refer to telindus24xx/profiles/atm/pvc_default/oamF5Loopback on page 377.

All entries in the vp configuration table are considered, even if for a certain VPI number no corresponding PVC has been configured. In the vp status and performance tables only the information about VPs that are configured in the vp configuration table is shown. However, the Telindus 2400 does respond to loop-back requests for VPs that are not configured in the vp configuration table but for which a PVC has been configured.

13.11 ATM switching configuration attributes

This section describes the following configuration attributes:

- telindus24xx/atm/switching on page 399

telindus24xx/atm/switching

Default:<empty>
Range: table, see below

Use this attribute to perform ATM switching. It is in this table that you have to specify which VCs and/or VPs you want to switch.

Note that on the ATM PVCs you want to switch the mode has to be set to switching. Refer to 11.3 - Configuring ATM switching on page 256 for more information.

The switching table contains the following elements:

Element	Description
sourceIntf	Use this element to enter the name of the (physical) source interface which carries the VC/VP that has to be switched. Default:<empty> Range: 0 … 24 characters
sourceVpi	Use this element to enter the VPI of the VC/VP that has to be switched. Default:0 Range: 0 … 7
sourceVci	Use this element to enter the VCI of the VC that has to be switched. Default:<opt> Range: 32 … 1024 In case of VP switching, leave this element to its default value (<opt>). Refer to What is VP switching? on page 257.
destinationIntf	Use this element to enter the name of the (physical) destination interface which carries the VC/VP when it has been switched. Default:<empty> Range: 0 … 24 characters
destinationVpi	Use this element to enter the new VPI of the VC/VP when it has been switched. Default:0 Range: 0 … 7
destinationVci	Use this element to enter the new VCI of the VC when it has been switched. Default:<opt> Range: 32 … 1024 In case of VP switching, leave this element to its default value (<opt>). Refer to What is VP switching? on page 257.
bidirectional	Use this element to determine whether the switching happens in both directions (bidirectional, i.e. from source to destination and vice versa) or only in one direction (unidirectional, i.e. only from source to destination). Default:yes Range: yes / no

13.12 Router configuration attributes

This section discusses the configuration attributes concerned with routing. First it describes the general routing configuration attributes such as defaultRoute, routingTable, etc. Then it explains the configuration attributes of the extra features such as address translation, L2TP tunnelling, filtering, IPSEC, etc.

The following gives an overview of this section:

- 13.12.1 - General router configuration attributes on page 401
- 13.12.2 - Default NAT configuration attributes on page 426
- 13.12.3 - L2TP tunnel configuration attributes on page 430
- 13.12.4 - Manual SA configuration attributes on page 438
- 13.12.5 - Routing filter configuration attributes on page 443

13.12.1 General router configuration attributes

This section describes the following configuration attributes:

- telindus24xx/ip/router/defaultRoute on page 402
- telindus24xx/ip/router/routingTable on page 403
- telindus24xx/ip/router/routingProtocol on page 404
- telindus24xx/ip/router/alternativeRoutes on page 405
- telindus24xx/ip/router/ripUpdateInterval on page 405
- telindus24xx/ip/router/ripHoldDownTime on page 406
- telindus24xx/ip/router/ripv2SecretTable on page 407
- telindus24xx/ip/router/sysSecret on page 408
- telindus24xx/ip/router/pppSecretTable on page 408
- telindus24xx/ip/router/helperProtocols on page 409
- telindus24xx/ip/router/sendTtlExceeded on page 410
- telindus24xx/ip/router/sendPortUnreachable on page 411
- telindus24xx/ip/router/sendAdminUnreachable on page 411
- telindus24xx/ip/router/dhcpStatic on page 412
- telindus24xx/ip/router/dhcpDynamic on page 413
- telindus24xx/ip/router/dhcpCheckAddress on page 415
- telindus24xx/ip/router/dns on page 418
- telindus24xx/ip/router/radius on page 415
- telindus24xx/ip/router/addrPools on page 419
- telindus24xx/ip/router/<alarmConfigurationAttributes> on page 425

telindus24xx/ip/router/defaultRoute

Default:-
Range: structure, see below

Use this attribute to set the default route. Refer to 9.3 - Configuring static routing on page 168 for more information on the default route.

The defaultRoute structure contains the following elements:

Element	Description
gateway	Use this element to specify the IP address of the next router that will route all packets for which no specific (static or dynamic) route exists in the routing table. Default:0.0.0.0 Range: up to 255.255.255.255 Whether you can omit the gateway element or not, is linked to the following conditions: **If the interface element specifies …** / **then ...** the LAN interface, / you can not omit the gateway element. the WAN interface, / you can omit the gateway element only when using PPP encapsulation. a DLCI, PVC or tunnel, / you can omit the gateway element.
interface	Use this element to specify the interface through which the gateway can be reached. Default:<empty> Range: 0 … 24 characters Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name). Note that this interface can also be a DLCI, PVC, tunnel, etc. If you do not specify a value for the interface element, then it is deduced by checking all interfaces (including DLCIs, PVCs and tunnels) and finding an interface for which the gateway lies in the subnet defined by the IP address and net mask of that interface. Typing the string “discard”, discards all packets for the corresponding destination.
preference	Use this element to set the level of importance of the default route with respect to routes learnt via RIP. Default:10 Range: 1 … 200 RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.
metric	Use this element to set with how much the metric parameter of a route has to be incremented. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. This element is only important when combining static routes and RIP routes. Refer to 9.5.3 - Explaining the rip structure on page 186 for more information on the metric parameter.

telindus24xx/ip/router/routingTable

Default:<empty>
Range: table, see below

Use this attribute to configure static routes. Refer to 9.3 - Configuring static routing on page 168 for more information on static routes.

The routingTable table contains the following elements:

Element	Description
network	Use this element to specify the IP address of the destination network. Default:0.0.0.0 Range: up to 255.255.255.255
mask	Use this element to specify the network mask of the destination network. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to specify the IP address of the next router on the path to the destination network. Default:0.0.0.0 Range: up to 255.255.255.255 Whether you can omit the gateway element or not, is linked to the following conditions: **If the interface element specifies …** / **then ...** the LAN interface, / you can not omit the gateway element. the WAN interface, / you can omit the gateway element only when using PPP encapsulation. a DLCI, PVC or tunnel, / you can omit the gateway element.
interface	Use this element to specify the interface through which the destination network can be reached. Default:<empty>
Range: 0 … 24 characters Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name on page 313). Note that the “interface” can also be a DLCI, PVC, tunnel, etc. If you do not specify a value for the interface element, then it is deduced by checking all interfaces (including DLCIs, PVCs and tunnels) and finding an interface for which the gateway lies in the subnet defined by the IP address and net mask of that interface. Typing the string “discard”, discards all packets for the corresponding destination.
preference	Use this element to set the level of importance of the route with respect to routes learnt via RIP. This element is only important when combining static routes and RIP routes. Default:10 Range: 1 … 200 RIP routes always have a preference of 60. Routes with a lower preference value are chosen over routes with higher preference value.

Element	Description
metric	Use this element to set with how much the metric parameter of a route has to be incremented. This element is only important when combining static routes and RIP routes. Default:1 Range: 1 … 15 If two routes exist with the same preference, then the route with the lowest metric value is chosen. Refer to 9.5.3 - Explaining the rip structure on page 186 for more information on the metric parameter.

telindus24xx/ip/router/routingProtocol

Default:none
Range: enumerated, see below

Use this attribute to activate or deactivate the Routing Information Protocol (RIP). Refer to 9.5 - Configuring the Routing Information Protocol on page 182 for more information on RIP.

The routingProtocol attribute has the following values:

Value	Description
none	No routing protocol is used. Only static routes are used.
rip	The RIP routing protocol is active. You can set the RIP version per interface. Refer to the elements txVersion and rxVersion in the rip structure (refer to 9.5.3 - Explaining the rip structure on page 186).

telindus24xx/ip/router/alternativeRoutes

Default:backup
Range: enumerated, see below

Use this attribute to determine how the Telindus 2400 deals with identical routes.

If more than one route to a (sub-)network is defined in the routing table, and these routes have …

- identical destination addresses, masks, preferences and metrics,
- a different gateway,

… then you can use the alternativeRoutes attribute to determine which route the Telindus 2400 uses to reach the (sub-)network.

The alternativeRoutes attribute has the following values:

Value	Description
backup	The Telindus 2400 always uses the same route to reach the (sub-)network. Only when this route goes down, it uses the alternative route.
roundRobin	The Telindus 2400 alternately uses the two possible routes to reach the (sub-)network. However, once a certain route is used to reach a specific address, this same route is always used to reach this specific address.

telindus24xx/ip/router/ripUpdateInterval

Default:00000d 00h 00m 30s
Range: 00000d 00h 00m 05s - 00000d 00h 10m 00s

Use this attribute to set the interval the Telindus 2400 transmits RIP update messages.

Normally, RIP update messages are transmitted every 30 seconds. It is possible to change this interval. However, changing this interval will also change the lifetime of routes learnt through RIP. If a RIP route is received for the last time, it is declared down after 6 times the ripUpdateInterval. After the route is down, it is deleted after 4 times the ripUpdateInterval.

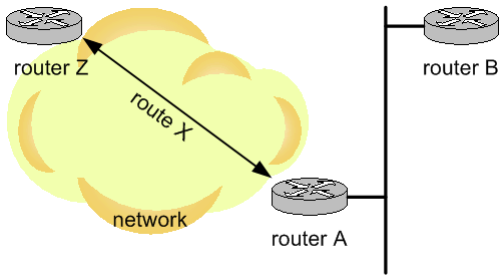
telindus24xx/ip/router/ripHoldDownTime

Default:00000d 00h 03m 00s
Range: 00000d 00h 00m 00s - 00000d 00h 10m 00s

Use this attribute to set the time the Telindus 2400 has to hold a route down in case it receives a RIP update message declaring this route down.

What is the RIP hold-down time?

Suppose you have a situation as depicted in the figure alongside.



Now suppose the following happens:

1. Route X goes down.
   ⇒Router A sends a RIP update message to router B declaring route X down.
2. Only a few moments later, route X goes up for a while after which it goes down again. This continues for a certain time. In other words, the route status toggles between up and down.
   ⇒Every time the status of route X changes, Router A sends a RIP update message to router B. Also router B propagates these RIP update messages. In other words, the toggling of route X causes that a lot of RIP update messages are sent.

The ripHoldDownTime attribute tries to avoid situations as described above. Suppose router B has a ripHoldDownTime attribute. In that case, the situation is as follows:

1. Route X goes down.
   ⇒Router A sends a RIP update message to router B declaring route X down. Router B starts the RIP hold-down timer.
2. The status of route X starts toggling between up and down.
   ⇒Router A sends several RIP update messages concerning route X to router B. Router B holds the status of route X down, as longs as the RIP hold-down timer has not expired.

When the RIP hold-down timer expires and the route is …

- down, then the route status stays down.
- up, then the route status changes to up.

telindus24xx/ip/router/ripv2SecretTable

Default:<empty>
Range: table, see below

Use this attribute to define the secrets used for the RIP authentication. Refer to 9.5.4 - Enabling RIP authentication on an interface on page 190 for more information on RIP authentication.

The ripv2SecretTable table contains the following elements:

Element	Description
keyId	Use this element to set a unique identifier for each secret. Default:0 Range: 0 … 255
secret	Use this element to define the secret. Default:<empty> Range: 0 … 16 characters This secret is sent with the RIP updates on the specified interface. It is also used to authenticate incoming RIP updates.
interface	Use this element to specify on which interface the secret is used. Default:all Range: 0 … 24 characters Do this by typing the name of the interface as you assigned it using the configuration attribute name (e.g. telindus24xx/lanInterface/name on page 313). Note that the “interface” can also be a DLCI, PVC, tunnel, etc. Entering the string “all” (default) means the secret is used on all the interfaces.

Remarks

- If authentication is enabled (either text or md5), then only updates using that authentication are processed. All other updates on that interface are discarded.
- If you use md5 and if for a certain interface multiple secrets are present in the ripv2SecretTable, then the first entry in the ripv2SecretTable is used to transmit RIP updates. Authentication of the received RIP updates is done by looking for the first secret with a matching key.
- If you use text and if for a certain interface multiple secrets are present in the ripv2SecretTable, then only the first entry in the ripv2SecretTable is used to transmit and receive RIP updates.

telindus24xx/ip/router/sysSecret

Default:<empty>
Range: 0 … 64 characters

Use this attribute for the PPP authentication process. The PPP authenticator uses the sysSecret attribute in order to verify the peer its response. For more information on PPP authentication, refer to …

- 7.2.6 - Configuring PAP on page 146
- 7.2.8 - Configuring CHAP on page 149

telindus24xx/ip/router/pppSecretTable

Default:<empty>
Range: table, see below

Use this attribute for the PPP authentication process. Enter the authentication name and secret of the remote router in this table. For more information on PPP authentication, refer to …

- 7.2.6 - Configuring PAP on page 146
- 7.2.8 - Configuring CHAP on page 149

The pppSecretTable contains the following elements:

Element	Description
name	Use this element to set the PPP authentication name of the remote router. Default:<empty> Range: 0 … 64 characters If the remote router is a Telindus 2400, then the name element should correspond with the remote Telindus 2400 its sysName or sessionName attribute.
secret	Use this element to set the PPP authentication secret of the remote router. Default:<empty> Range: 0 … 64 characters If the remote router is a Telindus 2400, then the secret element should correspond with the remote Telindus 2400 its sysSecret or sessionSecret attribute.

telindus24xx/ip/router/helperProtocols

Default:<empty>
Range: table, see below

Use this attribute to define the TCP and UDP port numbers for which broadcast forwarding is required. Use this attribute if you specified helper IP addresses using the helpers element in the ip structure of the LAN interface. Refer to 6.2.3 - Explaining the ip structure on page 90.

If the helperProtocols table is empty (default), then the following protocols are forwarded:

Protocol name	TCP/UDP port number
Time Server	37
IEN-116 Host Name Server	42
Domain Name Server	53
TACACS database service	65
Boot Protocol (BootP) / DHCP server	68
NetBIOS Name Server	137
NetBIOS Datagram Server	138

Important remarks

- Specifying at least one value in the helperProtocols table clears the default helper list automatically. In that case, if you want that for instance NetBios Datagram Server broadcast is forwarded, you have to specify port number 138 again.
- For BootP / DHCP broadcast packets, the Telindus 2400 is also a BootP / DHCP Relay Agent. If the protocol is selected, then the Telindus 2400 will write the IP address of its Ethernet interface in the BootP or DHCP gateway field and increment the hops field in addition to the address substitution.

telindus24xx/ip/router/sendTtlExceeded

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “TTL exceeded“ messages.

The sendTtlExceeded attribute has the following values:

Value	Description
enabled	The Telindus 2400 sends ICMP “TTL exceeded" messages.
disabled	The Telindus 2400 does not send ICMP “TTL exceeded” messages. This also implies that the router is not recognised by the UNIX or Windows trace-route feature.

What is Time To Live (TTL)?

Each IP packet has a Time To Live (TTL) value in its header. Each device that sends an IP packet sets this parameter at some fixed or predefined value. When the packet enters a router, the router decrements the TTL value. If a router finds a value 0 after decrementing the TTL, it discards the packet. This because a value 0 means the packet has passed too many routers. Probably the packet is looping between a number of routers. This mechanism avoids that routers with configuration errors bring down a complete network.

The ICMP message “TTL exceeded”

If a router discards a packet because its TTL is exceeded, it normally sends an ICMP “TTL exceeded“ message to the originator of the packet. With the sendTtlExceeded attribute you can define whether you want the Telindus 2400 to send such ICMP messages or not.

telindus24xx/ip/router/sendPortUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP “Destination unreachable: Port unreachable“ messages.

The sendPortUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 2400 sends ICMP “port unreachable" messages.
disabled	The Telindus 2400 does not send ICMP “port unreachable” messages. This also implies that the router is not recognised by the UNIX or Windows trace-route feature.

The ICMP message “port unreachable”

The Telindus 2400 supports a number of higher-layer IP protocols (Telnet, SNMP and TMA) for management purposes. If an IP packet is sent to the Telindus 2400 for a higher-layer protocol that it does not support, it normally sends an ICMP “Destination unreachable: Port unreachable“ message to the originator of the packet. With the sendPortUnreachable attribute you can define whether you want the Telindus 2400 to send such an ICMP message or not.

telindus24xx/ip/router/sendAdminUnreachable

Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the sending of ICMP "Destination unreachable: Communication with destination is administratively prohibited” messages.

The sendAdminUnreachable attribute has the following values:

Value	Description
enabled	The Telindus 2400 sends ICMP “communication prohibited“ messages.
disabled	The Telindus 2400 does not send ICMP “communication prohibited“ messages.

The ICMP message “communication prohibited”

If the Telindus 2400 receives an IP packet that is destined for a prohibited destination (because this destination is defined in an access list), then it sends an ICMP "Destination unreachable: Communication with destination is administratively prohibited” message to the originator of the packet. With this attribute you can define whether you want the Telindus 2400 to send such an ICMP message or not.

telindus24xx/ip/router/dhcpStatic

Default:<empty>
Range: table, see below

Use this attribute to assign a fixed IP address to an IP device and this for an infinite time.

The dhcpStatic table contains the following elements:

Element	Description
ipAddress	Use this element to assign an IP address to a certain client. This client is identified with its MAC address. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP address is specified, then there is no connection to the client. In that case, all other attributes in the table are ignored for this client.
mask	Use this element to set the client its subnet mask. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to set the default gateway for the client its subnet. Default:0.0.0.0 Range: up to 255.255.255.255 If no gateway is specified, then the gateway of the LAN channel is used.
nameServer	Use this element to set the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	Use this element to set the IP address of the TFTP server that is available to the client. It is the next server to use in boottrap. Default:0.0.0.0 Range: up to 255.255.255.255
macAddress	Use this element to enter the client its MAC address. Default:0.0.0.0.0.0 Range: up to ff.ff.ff.ff.ff.ff If no MAC address is specified, then there is no connection to the client. Therefore, all other attributes in the table are ignored for this client.
bootFile	Use this element to set the location of the boot file. Default:<empty> Range: 0 … 128 characters
hostName	Use this element to set the name of the client. Default:<empty> Range: 0 … 20 characters
domainName	Use this element to set the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: 0 … 20 characters
netbiosNameServer	Use this element to set the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC 1001 / RFC 1002. Default:<opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

telindus24xx/ip/router/dhcpDynamic

Default:<empty>
Range: table, see below

Use this attribute to assign an IP address selected from an IP address range to an IP device and this for a certain time.

The dhcpDynamic table contains the following elements:

Element	Description
ipStartAddress	Use this element to define the start address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 If no IP start address is specified, all other attributes on the same line in the table are ignored.
ipEndAddress	Use this element to define the end address of the IP address range. It is from this range that an IP address will be dynamically assigned to a client. Default:0.0.0.0 Range: up to 255.255.255.255 The IP address range will only contain the ipStartAddress in case … • no ipEndAddress is specified, • the specified ipEndAddress is the same as the ipStartAddress, • the specified ipEndAddress is smaller than the ipStartAddress, • the specified ipEndAddress belongs to another subnet than the ipStartAddress. Do not include the Telindus 2400 its own IP address in this range!
mask	Use this element to set the client its subnet mask for the specified IP address range. Default:255.255.255.0 Range: up to 255.255.255.255
gateway	Use this element to set the default gateway for the client its subnet. Default:0.0.0.0 Range: up to 255.255.255.255 If no gateway is specified, then the gateway of the LAN channel is used.
nameServer	Use this element to set the IP address of the name server that is available to the client. Default:0.0.0.0 Range: up to 255.255.255.255
tftpServer	Use this element to set the IP address of the TFTP server that is available to the client. It is the next server to use in boottrap. Default:0.0.0.0 Range: up to 255.255.255.255
leaseTime	Use this element to set the maximum time a client can lease an IP address from the specified IP address range. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s If 00000d 00h 00m 00s (default) is specified, then the lease time is infinite.
holdTime	Use this element to set the time between two consecutive leases of an IP address. I.e. if a client has just let go of its dynamically assigned IP address, then this same IP address can not be reassigned before the holdTime has elapsed. Default:00000d 00h 00m 00s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Element	Description
bootFile	Use this element to set the location of the boot file. Default:<empty> Range: 0 … 128 characters
hostName	Use this element to set the name of the client. Default:<empty> Range: 0 … 20 characters Because the DHCP server can not give the same name to all clients of this IP address range, a number is added to the host name from the second IP address onwards. The number goes up to 99. **Example** Suppose the host name is Telindus. In that case the name for the start IP address is Telindus, for the second IP address Telindus1, and so on.
domainName	Use this element to set the name the client should use when resolving hostnames via the Domain Name System (DNS). Default:<empty> Range: 0 … 20 characters
netbiosNameServer	Use this element to set the IP address of the NetBios server. Default:0.0.0.0 Range: up to 255.255.255.255
netbiosNodeType	Use this element to configure the client as described in RFC 1001 / RFC 1002. Default:<opt> Range: enumerated, see below The netbiosNodeType element has the following values: no-node, B-node, P-node, M-node, H-node.

DHCP server reaction on a BootP request

The DHCP server reacts on a BootP request as follows: the source MAC address of the incoming BootP request packet is compared with the MAC addresses that have been entered in the dhcpStatic table. Then, there are two possibilities:

- If the source MAC address corresponds with a MAC address in the dhcpStatic table, then the DHCP server replies with a BootP reply packet. In this reply, the IP address that is linked with the MAC address in question (as defined in the dhcpStatic table) is returned.
- If the source MAC address does not correspond with a MAC address in the dhcpStatic table, then the DHCP server returns no response on that frame.

Releasing IP addresses - DHCP versus BootP

On DHCP level, it is regularly checked whether the device that has an IP address in lease is still connected to the network. If it is not, the IP address is returned to the pool of free IP addresses.

On BootP level, however, such a check (or *refresh*) does not exist. What is more, a statistic IP address lease is for an infinite time. Consequently, if the device that requested the IP address is no longer connected to the network, this is not detected by the server. In that case, the statistical information will still indicate that the IP address is leased although it is not.

telindus24xx/ip/router/dhcpCheckAddress

Default:disabled
Range: enabled / disabled

Use this attribute to allow that the assigned IP address is probed with an ICMP Echo Request. This checks and prevents the double use of IP addresses.

The dhcpCheckAddress attribute has the following values:

Value	Description
enabled	No ICMP Echo Request is sent when an IP address is leased by a client.
disabled	An ICMP Echo Request is sent when an IP address is leased by a client. If an ICMP Echo Reply is received, it means the IP address is already in use. Therefore, another IP address is assigned.

telindus24xx/ip/router/radius

Default:-
Range: structure, see below

Use this attribute to configure the Telindus 2400 for RADIUS. Refer to What is RADIUS? on page 418.

To enable the use of RADIUS in PPP, CHAP or PAP should be enabled on the NAS (Network Access Server). The local configuration of the user name and password is ignored if a table of RADIUS servers exist. Furthermore, remote IP address and remote netmask are ignored if a RADIUS server forces these attributes.

The radius structure contains the following elements:

Element	Description
authServers	Use this element to select an authentication server. You can create a list of several authentication servers. Default:<empty> Range: table, see below The authServers table contains the following elements:

Element	Description
address	Use this element to specify the IP address of the authentication server. Default:0.0.0.0 Range: up to 255.255.255.255
secret	Use this element to set the authentication secret. Default:<empty> Range: 0 … 64 characters
timeOut	Use this element to specify the authentication time-out. Default:00000d 00h 00m 05s Range: 00000d 00h 00m 01s - 00000d 00h 00m 10s

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>acctServer</td><td>Use this element to select an accounting server. You can only select one accounting server.
Default:-
Range: structure, see below

The acctServer structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>address</td><td>Use this element to specify the IP address of the accounting server.
Default:0.0.0.0
Range: up to 255.255.255.255</td></tr>
<tr><td>secret</td><td>Use this element to set the accounting secret.
Default:<empty>
Range: 0 … 64 characters</td></tr>
<tr><td>timeOut</td><td>Use this element to specify the accounting time-out.
Default:00000d 00h 00m 05s
Range: 00000d 00h 00m 01s - 00000d 00h 00m 10s</td></tr>
</table>
</td></tr>
<tr><td>retries</td><td>Use this element to specify the number of retries before selecting the next authentication server in the authServers table.
Default:1
Range: 0 … 10</td></tr>
<tr><td>acctUpdate</td><td>Use this element to specify the time at which an update of the accounting data should be send to the server. Set this element to 0 (default) if no update is required.
Default:00000d 00h 00m 00s
Range: 00000d 00h 00m 00s - 00000d 00h 01m 00s

Note that this is not always supported by the accounting server.</td></tr>
</table>

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>login</td><td>Use this element to set the authentication of access to the Telindus 2400 using Telnet, FTP, TFTP or TMA. No accounting data is sent to the server.
Default:disabled
Range: enumerated, see below

The login element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>No RADIUS login authentication is done.</td></tr>
<tr><td>enabled</td><td>Login authentication is always done using a RADIUS server.

The user name and password have to be entered as follows: <code>"username:password"</code>. If the ‘:’ is omitted, then the string is considered to be a password.

Multiple passwords can be added using the same username. Access rights are sent using the RADIUS attribute CLASS (25) encoded as a string carrying a binary value. The bit definitions are:
• readAccess = 00000001B
• writeAccess = 00000010B
• securityAccess = 00000100B
• countryAccess = 00001000B (only used on aster4/5)
• fileAccess = 00010000B

Caution should be taken since all access to the device has to be authenticated by a RADIUS server.</td></tr>
<tr><td>fallback</td><td>Login authentication is done using a RADIUS server. If the server is not available, then authentication is done using the local security table of the device.</td></tr>
</table></td></tr>
<tr><td>ppp</td><td>Use this element to set the authentication of a PPP connection that uses CHAP or PAP.
Default:enabled
Range: enumerated, see below

The ppp element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled</td><td>PPP authentication is done using the local sysName/sysSecret or sessionName/sessionSecret of the device.</td></tr>
<tr><td>enabled</td><td>PPP authentication is always done using a RADIUS server.</td></tr>
</table></td></tr>
</table>

What is RADIUS?

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

telindus24xx/ip/router/dns

Default:-
Range: structure, see below

Use this attribute to enter the DNS server addresses. Refer to What is DNS? on page 418.

The dns structure contains the following elements:

Element	Description	
primaryDns	Use this element to specify the IP address of the primary DNS server.	Default:0.0.0.0 Range: up to 255.255.255.255
secondaryDns	Use this element to specify the IP address of the secondary DNS server.	Default:0.0.0.0 Range: up to 255.255.255.255
domainName	Use this element to enter the domain name to which the Telindus 2400 belongs.	Default:<empty> Range: 0 … 32 characters

What is DNS?

The Domain Name Service (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet however, is really based on IP addresses. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.mywebsite.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

telindus24xx/ip/router/addrPools

Default:<empty>
Range: table, see below

Use this attribute to create a list or an interval of IP addresses from which the Telindus 2400 can pick IP addresses and use them in its forwarding profiles.

The addrPool table contains the following elements:

Element	Description
name	Use this element to assign a name to the IP pool. Default:<empty> Range: 0 … 24 characters
pool	Use this element to select between an IP pool type and to add IP addresses to the pool. Default:<empty> Range: choice, see below You can select between the following IP pool types: • an IP list pool. Refer to telindus24xx/ip/router/addrPools/pool/list on page 420. • an IP interval pool. Refer to telindus24xx/ip/router/addrPool/pool/interval on page 423.

telindus24xx/ip/router/addrPools/pool/list

Default:<empty>
Range: table, see below

Use this table to create one or more lists of IP addresses from which the Telindus 2400 can pick IP addresses and use them as local and remote IP address of a link. Use the addrPool element in the ip structure to determine from which IP list pool the Telindus 2400 has to pick IP addresses. Refer to 6.2.3 - Explaining the ip structure on page 90 for more information.

The list table contains the following elements:

Element	Description
name	Use this element to assign a name to the IP list pool. Default:<empty> Range: 0 … 24 characters
pool	Use this element to create a list of IP addresses from which the Telindus 2400 can pick one. Default:<empty> Range: table, see below The pool table contains the following elements:

Element	Description
local	Use this element to set the local IP address. Default:0.0.0.0 Range: up to 255.255.255.255
remote	Use this element to set the remote IP address. Default:0.0.0.0 Range: up to 255.255.255.255
netmask	Use this element to set the subnet mask. Default:0.0.0.0 Range: up to 255.255.255.255

Important remark

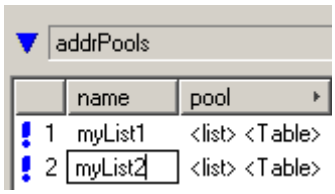
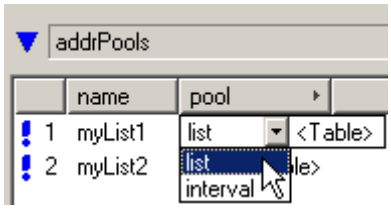
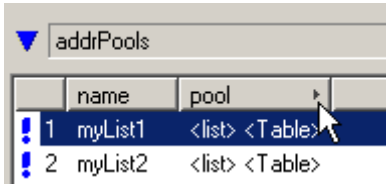
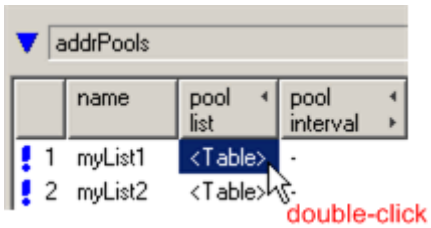
Note again that an IP list pool is for *both local and remote IP addresses*.

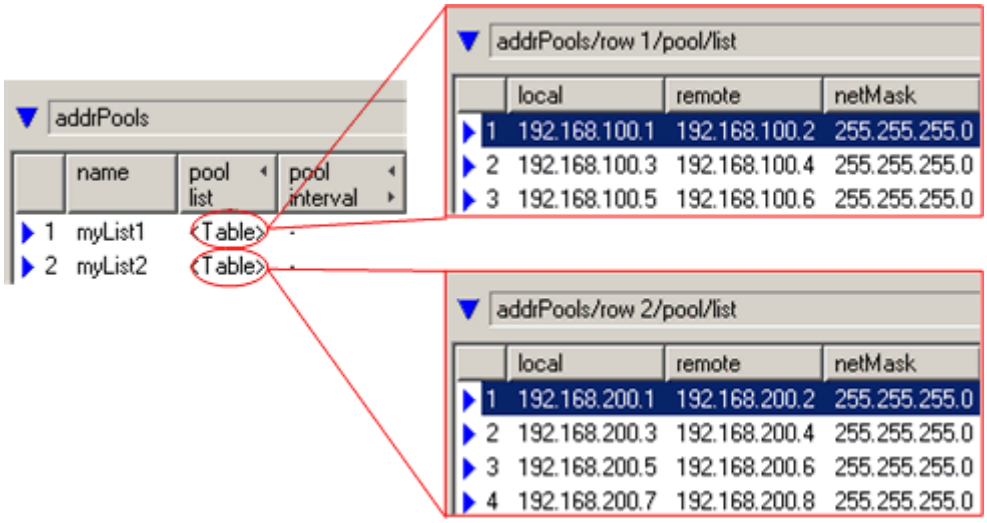
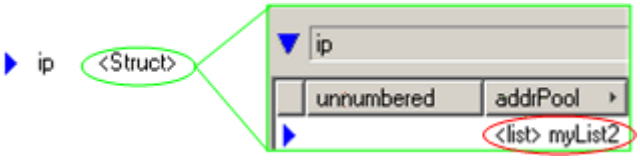
Example

Suppose …

- you want to create two IP list pools: myList1 and myList2.
- you want that the Telindus 2400 picks local and remote IP addresses from myList2.

Configure this as follows:

Step	Action
1	Create two entries in the ip/router/addrPools table and specify a name for each entry. 
2	In the pool element select the value list. 
3	Expand the pool element by clicking on the black triangle of the pool element. 
4	Double-click on the <Table> string situated in the pool/list column. 

Step	Action
5	Create entries in the pool/list tables and enter a local IP address, remote IP address and a netmask for each entry. 
6	In the addrPool element of the ip structure, select the value “list” and enter the name of the IP list pool from which you want to pick IP addresses. In our example, this is myList2. 

telindus24xx/ip/router/addrPool/pool/interval

Default:<empty>
Range: structure, see below

Use this structure to create one or more ranges of IP addresses from which the Telindus 2400 can pick IP addresses and use them as remote IP address of a link. Use the addrPool element in the ip structure to determine from which IP interval pool the Telindus 2400 has to pick IP addresses. Refer to 6.2.3 - Explaining the ip structure on page 90 for more information.

The interval structure contains the following elements:

Element	Description	
name	Use this element to assign a name to the IP interval pool.	Default:<empty> Range: 0 … 24 characters
from to	Use these elements to create a range of IP addresses from which the Telindus 2400 can pick one.	Default:0.0.0.0 Range: up to 255.255.255.255

Important remark

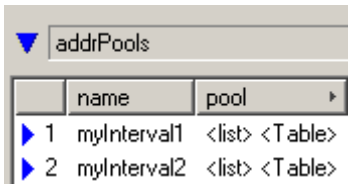
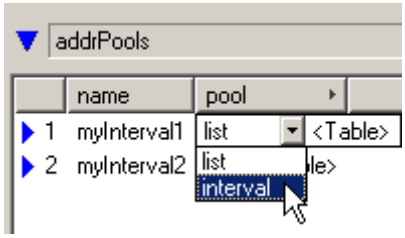
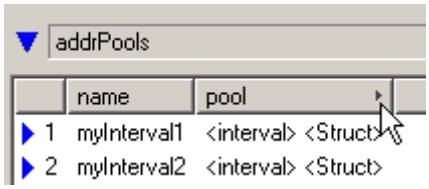
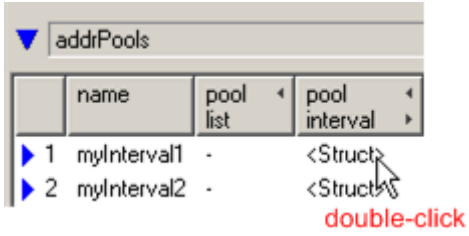
Note again that an IP interval pool is for *remote IP addresses only*.

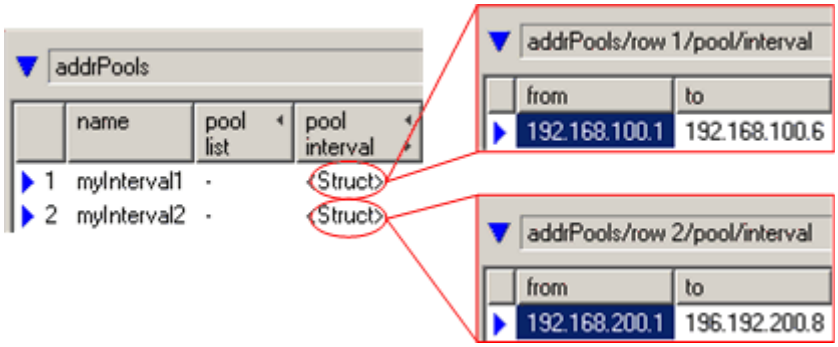
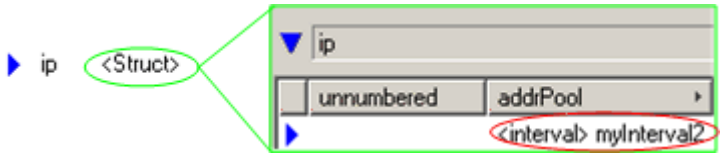
Example

Suppose …

- you want to create two IP interval pools: myInterval1 and myInterval2.
- you want that the Telindus 2400 picks a remote IP addresses from myInterval2.

Configure this as follows:

Step	Action
1	Create two entries in the ip/router/addrPools table and specify a name for each entry. 
2	In the pool element select the value interval. 
3	Expand the pool element by clicking on the black triangle of the pool element. 
4	Double-click on the <Struct> string situated in the pool/interval column. 

Step	Action
5	Configure the pool/interval structures. I.e. create an IP address range using the elements from and to. 
6	In the addrPool element of the ip structure, select the value “interval” and enter the name of the IP interval pool from which you want to pick IP addresses. In our example, this is myInterval2. 

telindus24xx/ip/router/<alarmConfigurationAttributes>

For more information on …

- the alarm configuration attributes alarmMask and alarmLevel and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the router object, refer to 16.9 - Router alarms on page 662.

13.12.2 Default NAT configuration attributes

This section describes the following configuration attributes:

- telindus24xx/ip/router/defaultNat/patAddress on page 427
- telindus24xx/ip/router/defaultNat/portTranslations on page 427
- telindus24xx/ip/router/defaultNat/servicesAvailable on page 428
- telindus24xx/ip/router/defaultNat/addresses on page 428
- telindus24xx/ip/router/defaultNat/gateway on page 428
- telindus24xx/ip/router/defaultNat/tcpSocketTimeOut on page 429
- telindus24xx/ip/router/defaultNat/udpSocketTimeOut on page 429
- telindus24xx/ip/router/defaultNat/tcpSockets on page 429
- telindus24xx/ip/router/defaultNat/udpSockets on page 429
- telindus24xx/ip/router/defaultNat/dmzHost on page 429

telindus24xx/ip/router/defaultNat/patAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to enter the official IP address that has to be used for the Port Address Translation. Entering an address different from the default value 0.0.0.0 automatically enables the general PAT process. Now you can activate or deactivate PAT per IP interface. Note that by default PAT is deactivated on all IP interfaces.

Refer to 9.6 - Configuring address translation on page 191 for more information on PAT.

telindus24xx/ip/router/defaultNat/portTranslations

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges that should not be translated when using PAT. Refer to 9.6.5 - PAT limitations and work-arounds on page 199.

Some TCP or UDP applications do not allow port translations: these applications require a dedicated source port number. In the portTranslations table you can define UDP and TCP port ranges that should not be translated. If a packet with a source port number in such a range is received, PAT replaces only the source IP address provided it is the first device using this port number. When other devices using the same application (hence the same port number) try to send traffic to the same Internet destination address, PAT discards this traffic. It is also possible to define port ranges that PAT should always discard. The port translation range PAT uses goes from 60928 up to 65535.

The portTranslations table contains the following elements:

Element	Description
protocol	Use this element to select the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	Use this element to set the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	Use this element to set the highest value of the TCP or UDP port range. Default:<opt> Range: 0 … 65535 If no endPort value is defined (<opt>), then the port range is limited to the startPort value only.
action	Use this element to set the action in case a packet is received with a source port number that falls within the specified port range. Default:noTranslation Range: enumerated, see below The action element has the following values:

Value	Description
noTranslation	The port numbers that fall within the specified port range are not translated.
deny	Packets with port numbers that fall within the specified port range are discarded.

telindus24xx/ip/router/defaultNat/servicesAvailable

Default:<empty>
Range: table, see below

Use this attribute to define specific port number ranges for incoming Internet traffic that should not be translated when using PAT. Instead it is sent to the corresponding private IP address. Refer to 9.6.5 - PAT limitations and work-arounds on page 199.

The servicesAvailable table makes it possible to have a server on the local network that can be accessed from the Internet, although it has no official IP address.

The servicesAvailable table contains the following elements:

Element	Description
protocol	Use this element to select the protocol: tcp or udp. Default:tcp Range: tcp / udp
startPort	Use this element to set the lowest value of the TCP or UDP port range. Default:0 Range: 0 … 65535
endPort	Use this element to set the highest value of the TCP or UDP port range. Default:<opt> Range: 0 … 65535 If no endPort value is defined (<opt>), then the port range is limited to the startPort value only.
serverAddress	Use this element to set the private server address. Default:0.0.0.0 Range: up to 255.255.255.255 If a packet is received with a source port number that falls within the specified port range, then it is sent to the private server address.

telindus24xx/ip/router/defaultNat/addresses

Default:<empty>
Range: table, see below

Use this attribute to enter all the official IP addresses that have to be used for Network Address Translation. Entering an address in the addresses table automatically enables the general NAT process. Now you can activate or deactivate NAT per IP interface. Note that by default NAT is deactivated on all IP interfaces.

Refer to 9.6 - Configuring address translation on page 191 for more information on NAT.

The addresses table contains the following elements:

Element	Description
officialAddress	Use this element to set the official IP address. These addresses are used in the reverse order as they appear in the list.
privateAddress	Use this element to set the private IP address, i.e. to permanently assign an official IP address to a private address.

telindus24xx/ip/router/defaultNat/gateway

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to define the gateway addresses from routes on which address translation should be applied. If you do not configure the gateway attribute, then the ip/router/defaultRoute attribute is taken as only gateway addresses.

telindus24xx/ip/router/defaultNat/tcpSocketTimeOut

Default:00001d 00h 00m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for TCP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for one day by default. Only decrease this attribute if some TCP applications do not close properly, filling up the available translation sessions.

telindus24xx/ip/router/defaultNat/udpSocketTimeOut

Default:00000d 00h 03m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to define the time-out for UDP sessions that are not closed by the application.

Such sessions, whether PAT or NAT is in use, remain active for 3 minutes by default. Only decrease this attribute if some UDP applications do not close properly, filling up the available translation sessions.

telindus24xx/ip/router/defaultNat/tcpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of TCP session that may be used simultaneously for address translation.

telindus24xx/ip/router/defaultNat/udpSockets

Default:1024
Range: 500 … 4500

Use this attribute to set the maximum number of UDP session that may be used simultaneously for address translation.

telindus24xx/ip/router/defaultNat/dmzHost

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to set the address of the DMZ (demilitarised zone) host.

What is a DMZ host?

In computer networks, a DMZ (demilitarised zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed.

13.12.3 L2TP tunnel configuration attributes

This section describes the following configuration attributes:

- telindus24xx/ip/router/tunnels/l2tpTunnels on page 431
- telindus24xx/ip/router/tunnels/ipsecL2tpTunnels on page 436

telindus24xx/ip/router/tunnels/l2tpTunnels

Default:<empty>
Range: table, see below

Use this attribute to configure the Layer 2 Tunnelling Protocol tunnels you want to set up. Add a row to the l2tpTunnels table for each L2TP tunnel you want to set up.

The l2tpTunnels table contains the following elements:

Element	Description
name	Use this element to assign an administrative name to the tunnel. Default:<empty> Range: 0 … 24 characters
adminStatus	Use this element to activate (up) or deactivate the tunnel (down). Default:down Range: up / down
mode	Use this element to determine whether for the corresponding tunnel, IP packets are treated by the routing process, the bridging process or both. Default:routing Range: enumerated, see below The mode element has the following values:
ip	Use this element to configure the IP related parameters of the tunnel. Default:- Range: structure, see below Building an L2TP tunnel is based on logical interfaces. Those logical interfaces have their own IP address. Refer to … • 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses. • 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.

Value	Description
bridging	All packets received on the tunnel are bridged.
routing	All packets received on the tunnel are routed.
routingAndBridging	The SNAP header is checked to determine whether the packets have to be bridged or routed.

Element	Description
bridging	Use this element to configure the bridging related parameters of the tunnel in case the mode attribute is set to bridging or routingAndBridging. Default:- Range: structure, see below When bridging is enabled on a tunnel interface, the tunnel acts exactly as a bridge port for a physical PPP connection. Refer to … • 10 - Configuring bridging on page 223 for more information on bridging. • 10.2.6 - Explaining the bridging structure on page 241 for a detailed description of the bridging structure.
l2tp	Use this element to configure the L2TP related parameters of the tunnel. Default:- Range: structure, see below Refer to telindus24xx/ip/router/tunnels/l2tpTunnels/l2tp on page 433 for a detailed description of the l2tp structure.

Remarks

- L2TP tunnels can also be set up by an IP host. The Telindus 2400 is transparent for tunnels set up by a host.
- Multiple L2TP tunnels are possible on a single link. Multiple PPP sessions are possible within a single L2TP tunnel.

telindus24xx/ip/router/tunnels/l2tpTunnels/l2tp

Default:-
Range: structure, see below

Use this structure to configure the specific L2TP related parameters of the tunnel.

The l2tp structure contains the following elements:

Element	Description
localIpAddress	Use this element to set the official IP address that serves as start point of the L2TP connection. Default:<opt> Range: up to 255.255.255.255
remoteIpAddress	Use this element to set the official IP address that serves as end point of the L2TP connection. Default:<opt> Range: up to 255.255.255.255 Both localIpAddress and remoteIpAddress together with the well-known port number for L2TP (i.e. 1701), make up the socket used for the L2TP session. At the moment, only one L2TP session can exist between one localIpAddress and remoteIpAddress combination.
pppAuthentication	Use this element to enable or disable PPP authentication on the PPP link in the tunnel. Default:disabled Range: enumerated, see below The pppAuthentication element has the following values: **Value** / **Description** disabled — Authentication is disabled. pap — This side of the link requests a PAP authentication from the remote router. chap — This side of the link requests a CHAP authentication from the remote router. chapOrPap — This side of the link requests a CHAP or PAP authentication from the remote router. If the remote router supports … • only PAP, then PAP is used. • only CHAP, then CHAP is used. • both CHAP and PAP, then CHAP is used. Refer to … • 7.2.6 - Configuring PAP on page 146 for more information on PAP. • 7.2.8 - Configuring CHAP on page 149 for more information on CHAP.
pppSessionName	Use this element to set the PPP session name. This is then used in the PPP authentication process. The PPP authenticator uses the pppSessionName element in order to verify the peer its response. Default:<empty> Range: 0 … 64 characters
pppSessionSecret	Use this element to set the PPP session secret. This is then used in the PPP authentication process. The PPP authenticator uses the pppSessionSecret element in order to verify the peer its response. Default:<empty> Range: 0 … 64 characters

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>type</td><td>Use this element to specify the tunnel type.
Default:outgoingDial
Range: enumerated, see below

The type element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>outgoingDial</td><td>The outgoing tunnel is not continuously open. It is opened whenever data has to be sent through the tunnel, and closed when no data is detected for a certain time.</td></tr>
<tr><td>outgoingLeasedLine</td><td>The outgoing tunnel is opened as soon as the Telindus 2400 is up, and it stays open.</td></tr>
<tr><td>incoming</td><td>The tunnel is an incoming tunnel.</td></tr>
</table></td></tr>
<tr><td>dataChannelSequenceNumbering</td><td>Use this element to enable (on) or disable (off) sequence numbering on the data messages. These sequence numbers are used to detect lost packets and/or restore the original sequence of packets that may have been reordered during transport.
Default:off
Range: on / off

On control messages, sequence numbering is always enabled.

It is recommended that for connections where reordering or packet loss may occur, dataChannelSequenceNumbering is enabled.</td></tr>
<tr><td>keepAliveTimeOut</td><td>Use this element to set the amount of time (in seconds) the tunnel waits before it sends a keep alive message in case it receives no data.
Default:30
Range: 1 ... 3600

If the tunnel does not receive incoming data during a certain time, it sends a keep alive message to the other side and waits for an acknowledgement.</td></tr>
<tr><td>mode</td><td>Use this element to set the L2TP mode of the Telindus 2400.

The mode element has the following values:

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>lac</td><td>The Telindus 2400 acts as an L2TP Access Concentrator.</td></tr>
<tr><td>lns</td><td>The Telindus 2400 acts as an L2TP Network Server.</td></tr>
<tr><td>auto</td><td>If both local and remote Telindus 2400 are set to auto, they mutually decide who will be the LAC and who the LNS.</td></tr>
</table>

Select auto only if you use a Telindus router at both sides of the tunnel. In conjunction with routers from other vendors (e.g. Cisco), specifically select an L2TP mode (lac or lns).</td></tr>
</table>

Element	Description
tunnelAuthentication	Use this element to enable (on) or disable (off) tunnel authentication. Default:off Range: on / off L2TP incorporates a simple, optional, CHAP-like tunnel authentication system during control connection establishment. If the LAC or LNS wishes to authenticate the identity of the peer it is contacting or being contacted by, it sends a challenge packet. If the expected response and response received from a peer does not match, the tunnel is not opened. To participate in tunnel authentication, a single shared secret has to exist between the LAC and LNS.
tunnelSecret	Use this element to set the tunnel secret. This secret is used in the tunnel authentication in order to verify the peer its response. Default:<empty> Range: 0 … 64 characters
copyTos	Use this element to enable (on) or disable (off) the copying of the TOS byte value of the packets. Default:on Range: on / off
maxNrOfRetransmissions	Use this element to set the number of times a control message has to be retransmitted in case no acknowledgement follows. If after the configured number of times (default 4) still no acknowledgement is received, then the tunnel is closed. Default:4 Range: 0 … 10
transmitWindowSize	Use this element to set the window size for transmitting control messages. Default:4 Range: 1 … 30
receiveWindowSize	Use this element to set the window size for receiving control messages. Default:4 Range: 1 … 30
udpChecksum	Use this element to enable (on) or disable (off) the UDP checksum. Default:off Range: on / off It is recommended to enable the UDP checksum on lower quality links.
calledNr	Use this element to set the called number. Default:<empty> Range: 0 … 48 characters The called number is an indication to the receiver of a call as to what (telephone) number the caller used to reach it. It encodes the (telephone) number to be called for an outgoing call request (OCRQ) and the called number for an incoming call request (ICRQ). The called number is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value needed in this element.
speed	Use this element to make an indication of the expected speed for the tunnel in case of MLPPP. Default:64000 Range: 0 … 2147483647

telindus24xx/ip/router/tunnels/ipsecL2tpTunnels

Default:<empty>
Range: table, see below

Use this attribute to configure the IP secured Layer 2 Tunnelling Protocol tunnels you want to set up. Add a row to the IpsecL2tpTunnels table for each IPSEC L2TP tunnel you want to set up.

The elements of the ipsecL2tpTunnel are basically the same as the elements of the l2tpTunnel (refer to telindus24xx/ip/router/tunnels/l2tpTunnels on page 431). The only difference is the presence of the ipsec element within the l2tp structure. Refer to telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/l2tp/ipsec on page 436 for more information on the ipsec element.

telindus24xx/ip/router/tunnels/ipsecL2tpTunnels/l2tp/ipsec

Default:-
Range: choice, see below

Use this element to apply a security association to the IPSEC L2TP tunnel.

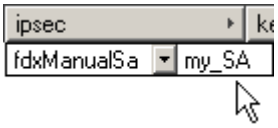
The ipsec element offers you the following choice:

Choice	Description
fdxManualSa	Select this value when you want to apply a security association to both the inbound and outbound traffic of the IPSEC L2TP tunnel. Default:<empty> Range: 0 … 24 characters If you select this value, then a field appears behind the value. Type the manualSA object its index name in this field. See below for more information on applying a security association.
hdxManualSa	Select this value when you want to apply a security association to the inbound traffic and another security association outbound traffic of the IPSEC L2TP tunnel. Default:- Range: structure, see below If you select this value, then a structure appears behind the value. This structure contains the following elements: **Element** / **Description** inbound: To apply a security association on the inbound traffic, type the manualSA object its index name in this field. outbound: To apply a security association on the outbound traffic, type the manualSA object its index name in this field. See below for more information on applying a security association.

You can apply a security association on the IPSEC L2TP tunnel by typing the index name of the security association you want to use. You can create the security association itself by adding a manualSA object under the router object and by configuring the attributes in this object.

Example

If you created a manualSA object with index name my_SA (i.e. manualSA[my_SA]) and you want to apply this security association here, then enter the index name as value for the ipsec element.



Refer to …

- 12.5 - Configuring IP security on page 289 for more information on IP security.
- 4.4 - Adding an object to the containment tree on page 56 for more information on adding objects.

13.12.4 Manual SA configuration attributes

This section describes the following configuration attributes:

- telindus24xx/ip/router/manualSA[ ]/espEncryptionAlgorithm on page 439
- telindus24xx/ip/router/manualSA[ ]/espEncryptionKey on page 440
- telindus24xx/ip/router/manualSA[ ]/espAuthenticationAlgorithm on page 441
- telindus24xx/ip/router/manualSA[ ]/espAuthenticationKey on page 441
- telindus24xx/ip/router/manualSA[ ]/spi on page 442

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/ip/router/manualSA[ ]/espEncryptionAlgorithm

Default:des
Range: enumerated, see below

Use this attribute to select the algorithm that will be used to encrypt the data when using IPSEC.

The espEncryptionAlgorithm attribute has the following values:

Value	Description
null	No encryption is done. The null encryption algorithm is simply a convenient way to represent the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.
des	DES is used to encrypt / decrypt the data. The DES key has to be entered in the espEncryptionKey attribute.
3des	Triple DES is used to encrypt / decrypt the data. The 3DES key has to be entered in the espEncryptionKey attribute. When using 3DES, the first 8 octets are used to encrypt the data, the

Make sure that for the same security association on both the local and remote router the same ESP encryption algorithm is selected.

telindus24xx/ip/router/manualSA[ ]/espEncryptionKey

Default:<empty>
Range: octet string, 0 … 24

Use this attribute to define the key that will be used in the encryption / decryption process when using IPSEC. The algorithm can be selected using the espEncryptionAlgorithm attribute.

If you use …	then …
null encryption	the setting of the espEncryptionKey attribute is irrelevant.
DES encryption	only the first 8 octets of the key are used. All other octets are ignored. 11 11 11 11 11 11 11 11 22 22 22 22 22 22 22 22 33 33 33 33 33 33 33 33 used in the encryption / decryption process not used in the encryption / decryption process
3DES encryption	at the transmitter side, the first set of 8 octets of the key are used to encrypt the data, the second set of 8 octets to decrypt the data and the third set of 8 octets to encrypt the data again. 11 11 11 11 11 11 11 11 22 22 22 22 22 22 22 22 33 33 33 33 33 33 33 33 encryption decryption encryption At the receiver side, the opposite occurs.

Make sure that for the same security association on both the local and remote router the same ESP encryption key is used.

telindus24xx/ip/router/manualSA[ ]/espAuthenticationAlgorithm

Default:hmac_md5
Range: enumerated, see below

Use this attribute to select the algorithm that will be used to authenticate the data when using IPSEC.

The espAuthenticationAlgorithm attribute has the following values:

Value	Description
null	No authentication is done.
hmac_md5	The MD5 hash function is used to authenticate the data. The MD5 key has to be entered in the espAuthenticationKey attribute.
hmac_sha-1	The SHA-1 hash function is used to authenticate the data. The SHA-1 key has to be entered in the espAuthenticationKey attribute.

Make sure that for the same security association on both the local and remote router the same ESP authentication algorithm is selected.

telindus24xx/ip/router/manualSA[ ]/espAuthenticationKey

Default:<empty>
Range: octet string, 0 … 20

Use this attribute to define the key that will be used in the authentication process when using IPSEC. The algorithm can be selected using the espAuthenticationAlgorithm attribute.

If you use …	then …
null authentication	the setting of the espAuthenticationKey attribute is irrelevant.
MD5 authentication	only the first 16 octets of the key are used. All other octets are ignored. 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 used in the authentication process not used in the authentication process
SHA-1 authentication	all 20 octets of the key are used.

Make sure that on both the local and remote router the same ESP authentication key is used.

telindus24xx/ip/router/manualSA[ ]/spi

Default:256
Range: 256 ... 2147483647

Use this attribute to set the SPI value. Each security association must have a unique SPI value because this value is used to identify the security association.

Make sure that for the same security association on both the local and remote router the same SPI value is used.

13.12.5 Routing filter configuration attributes

This section describes the following configuration attributes:

- telindus24xx/ip/router/routingFilter[ ]/filter on page 444

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/ip/router/routingFilter[ ]/filter

Default:<empty>
Range: table, see below

Use this attribute to set up a routing update filter.

Only the routes to networks that are specified in the filter table are forwarded. All other routes are blocked. If the filter table is empty, then all routes are forwarded.

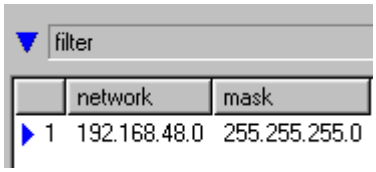
The filter table contains the following elements:

Element	Description
network	This is the IP address of the network. The address may be a (sub-)network address. It should match an entry in the telindus24xx/ip/router/routingTable status attribute of the Telindus 2400. Default:0.0.0.0 Range: up to 255.255.255.255
mask	This is the IP subnet mask of the network. By combining an IP address with a mask you can uniquely identify a range of addresses. Default:255.255.255.0 Range: up to 255.255.255.255

Currently, the Telindus 2400 supports up to 5 routing update filters. Although you can add more than 5 routingFilter[ ] objects to the containment tree, no more than 5 will be active.

Example

This example shows a filter that only forwards the route to subnet 192.168.48.0.



13.13 Bridge configuration attributes

This section discusses the configuration attributes concerned with bridging. First it describes the general bridging configuration attributes such as spanningTree, etc. Then it explains the configuration attributes of the extra features such as bridge access lists, etc…

The following gives an overview of this section:

- 13.13.1 - Bridge group configuration attributes on page 446
- 13.13.2 - Bridge access list configuration attributes on page 454

13.13.1 Bridge group configuration attributes

This section describes the following configuration attributes:

- telindus24xx/bridge/bridgeGroup/name on page 447
- telindus24xx/bridge/bridgeGroup/ip on page 447
- telindus24xx/bridge/bridgeGroup/arp on page 447
- telindus24xx/bridge/bridgeGroup/bridgeCache on page 448
- telindus24xx/bridge/bridgeGroup/bridgeTimeOut on page 449
- telindus24xx/bridge/bridgeGroup/spanningTree on page 449
- telindus24xx/bridge/bridgeGroup/localAccess on page 450
- telindus24xx/bridge/bridgeGroup/macAddress on page 451
- telindus24xx/bridge/bridgeGroup/vlan on page 451
- telindus24xx/bridge/bridgeGroup/vlanSwitching on page 452

telindus24xx/bridge/bridgeGroup/name

Default:bridge
Range: 1 … 24 characters

Use this attribute to assign an administrative name to the bridge group.

This attribute is only present on the default bridge group (bridgeGroup), not on the user instantiatable bridge groups (vpnBridgeGroup[ ]). The user instantiatable bridge groups their name is the index name that you have to specify when you add the bridge group object to the containment tree (refer to 10.2.3 - Adding a bridge group on page 237).

telindus24xx/bridge/bridgeGroup/ip

Default:<empty>
Range: structure, see below

Use this attribute to configure the IP related parameters of the bridge group.

Refer to …

- 6.2 - Configuring IP addresses on page 87 for general information on configuring IP addresses.
- 6.2.3 - Explaining the ip structure on page 90 for a detailed description of the ip structure.

Important remark

If you set the configuration attribute telindus24xx/lanInterface/mode to bridging, then the settings of the configuration attribute telindus24xx/lanInterface/ip are ignored. As a result, if you want to manage the Telindus 2400 via IP, you have to configure an IP address in the bridgeGroup object instead: telindus24xx/bridge/bridgeGroup/ip.

telindus24xx/bridge/bridgeGroup/arp

Default:-
Range: structure, see below

Use this attribute to configure the Address Resolution Protocol (ARP) cache of the bridge group.

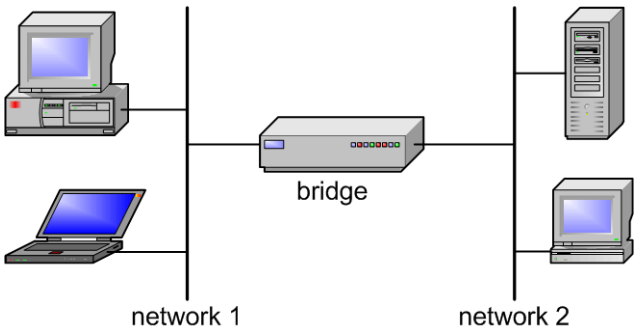
Refer to telindus24xx/lanInterface/arp on page 314 for a detailed description of the arp structure.

telindus24xx/bridge/bridgeGroup/bridgeCache

Default:learning
Range: enumerated, see below

Use this attribute to determine how the bridge group should act: as a repeater, a filter or a switch.

The bridgeCache attribute has the following values:

Value	Description
disabled	The bridge group acts as a repeater. All the data which originates from network 1 will be let through to network 2. Even if the data is not destined for that network. 
learning	The bridge group acts as a filter. Data coming from network 1, will only be let through by the bridge if this data has a destination outside network 1 or if it has a broadcast or multicast address. This means the bridge filters the data and decreases the amount of data traffic on the separated LAN segments.
switching	The bridge group acts as a VLAN switch. VLANs on network 1 are switched to VLANs on network 2. Use the vlanSwitching attribute to specify which VLANs you want to switch. Refer to … • telindus24xx/bridge/bridgeGroup/vlanSwitching on page 452 • 11.2 - Configuring VLAN switching on page 251

What is the bridge cache?

Whereas the ARP cache keeps MAC address - IP address pairs, the bridge cache (also called address database) keeps MAC address - interface pairs. This allows the bridge to know which device is reachable through which interface. Refer to telindus24xx/bridge/bridgeGroup/bridgeCache on page 565 for an example of such a table.

telindus24xx/bridge/bridgeGroup/bridgeTimeOut

Default:00000d 00h 05m 00s
Range: 00000d 00h 00m 00s-
24855d 03h 14m 07s

Use this attribute to set the ageing time of the bridge cache entries.

The bridge cache time-out

If devices on the network are (re)moved then the MAC address - interface relation changes (refer to What is the bridge cache?). Therefore, the bridge cache entries are automatically removed from the cache after a fixed time-out. This time-out period can be set with the bridgeTimeOut attribute. This in case no topology change is detected, otherwise the time-out is equal to the value of the bridgeForwardDelay element of the spanningTree attribute.

When checking the bridgeCache it may appear that some entries are present for a longer time than is configured with the bridgeTimeOut attribute. This because the entries in the bridgeCache are not monitored continuously, but once per minute. As a result, some entries may appear to be “overtime”. However, this should be no more than ± 75 seconds.

telindus24xx/bridge/bridgeGroup/spanningTree

Default:-
Range: structure, see below

Use this attribute to configure the bridging related parameters of the bridge group.

Whereas the bridging attribute groups the bridging related parameters per interface, the spanningTree attribute groups the bridging related parameters of the bridge as a whole.

The spanningTree structure contains the following elements:

Element	Description
protocol	Use this element to select the bridging protocol. Default:none Range: enumerated, see below The protocol element has the following values: **Value** / **Description** none: The Telindus 2400 uses the self-learning principle. This means that the bridge itself learns which data it has to forward and which data it has to block. I.e. it builds its own bridging table. p802.1D: The Telindus 2400 uses the self-learning principle in conjunction with the Spanning Tree protocol. Because Spanning Tree bridging is somewhat more complicated than self-learning bridging, an introduction is given in 10.1.2 - The self-learning and Transparent Spanning Tree bridge on page 226. When using ATM encapsulation together with the Spanning Tree protocol, every PVC is considered as a separate bridge port. So each PVC is than considered as a special kind of LAN with only both end points connected.

Element	Description
bridgePriority	Use this element to set the priority of the bridge. Default:32768 Range: 0 … 65535 The bridge its MAC address together with the bridgePriority element form a unique bridge identifier. This identifier is used to determine which bridge becomes the root bridge. The bridge with the lowest bridgePriority value becomes the root bridge. If two bridges have the same bridgePriority value, then the bridge with the lowest MAC address becomes the root bridge.
bridgeMaxAge	Use this element to set the time the bridge retains bridging information before discarding it. Default:00000d 00h 00m 20s Range: 00000d 00h 00m 06s - 00000d 00h 00m 40s
bridgeHelloTime	Use this element to set the interval by which the root bridge sends Configuration BPDUs, also called Hello messages. Default:00000d 00h 00m 02s Range: 00000d 00h 00m 01s - 00000d 00h 00m 10s
bridgeForwardDelay	Use this element to set … Default:00000d 00h 00m 15s Range: 00000d 00h 00m 04s - 00000d 00h 00m 30s • the delay a bridge port applies to move from listening state to learning state or from learning state to forwarding state. Refer to 10.1.5 - The Spanning Tree bridge port states on page 229 for more information on the possible states of a bridge port. • the time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected.

telindus24xx/bridge/bridgeGroup/localAccess

Default:permitted
Range: enumerated, see below

Use this attribute to allow or deny access to the bridge group itself.

The localAccess attribute has the following values:

Value	Description
permitted	Bridged packets can be delivered to the bridge group itself.
restricted	No bridged packets can be delivered to the bridge group itself. This adds some security, because the Telindus 2400 can not be accessed through the bridge group. You could for instance create one bridge group specifically for … • management purposes. In this bridge group, set the localAccess attribute to permitted. • the actual data coming from the customers. In this bridge group, set the localAccess attribute to restricted. In this way, de customer can never access the Telindus 2400 itself.

telindus24xx/bridge/bridgeGroup/macAddress

Default:<deviceMac> lan
Range: choice, see below

Use this attribute to determine whether a fixed, a random or a user defined MAC address is associated with the bridge group.

The macAddress attribute has the following values:

Value	Description
deviceMac	A MAC address from the Telindus 2400 itself is associated with the bridge group. Use the second part of the macAddress attribute to define which MAC address has to be selected: **Value** / **Description** lan: The LAN interface its MAC address is associated with the bridge group. random: The Telindus 2400 generates a random MAC address and this is associated with the bridge group
userMac	A user defined MAC address is associated with the bridge group. Use the second part of the macAddress attribute to enter the MAC address.

telindus24xx/bridge/bridgeGroup/vlan

Default:-
Range: structure, see below

Use this attribute to configure some VLAN (IEEE 802.1Q) related parameters of the bridge group in case you want to manage the Telindus 2400 over a VLAN.

Although the Telindus 2400 bridges VLAN tagged frames when connected to a VLAN aware switch, the Telindus 2400 itself can only be managed via IP if some VLAN parameters are configured in the bridgeGroup/vlan structure.

The vlan structure contains the following elements:

Element	Description
dotQTagging	Use this element to enable or disable … • the VLAN tagging of Ethernet frames sent by the Telindus 2400. • the recognition of VLAN tagged Ethernet frames received by the Telindus 2400. Default:disabled Range: enabled / disabled
vid	Use this element to set the VLAN ID over which the Telindus 2400 can be managed. Default:1 Range: 1 … 4094
userPriority	Use this element to set the user priority in the VLAN tag and this for all frames sent by the Telindus 2400. Default:0 Range: 0 … 7

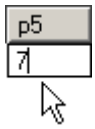
telindus24xx/bridge/bridgeGroup/vlanSwitching

Default:<empty>
Range: table, see below

Use this attribute specify which VLANs you want to switch in case the bridge group is used as a VLAN switch. Note that you have to enable VLAN switching on the bridge group by setting the bridgeCache attribute to switching. Refer to …

- telindus24xx/bridge/bridgeGroup/bridgeCache on page 448
- 11.2 - Configuring VLAN switching on page 251

The vlanSwitching attribute contains the following elements:

Element	Description
sourceIntf	Use this element to enter the name of the (physical) source interface which carries the VLAN that has to be switched. Default:<empty> Range: 0 … 24 characters
sourceVlan	Use this element to enter the VLAN ID of the VLAN that has to be switched. Default:1 Range: 0 … 4094 **Stripping the VLAN tag** Entering 0 as VLAN ID strips the VLAN tag of the Ethernet frame. Example: suppose you enter 1 as srcVlan and 0 as dstVlan. So VLAN 1 is switched from the source interface to the destination interface. But before it is sent out on the destination interface, the VLAN tag is stripped. So instead of VLAN tagged Ethernet frames, plain Ethernet frames are sent out. In the opposite direction however, the VLAN tag is added again.
sourcePMap	Use this element to, if desired, remap the VLAN priorities. Since the switching is bidirectional, you can remap priorities for both directions (i.e. both at the “source” and “destination” interface). Default:- Range: structure, see below The structure contains the elements p0 up to p7, which represent priority 0 up to priority 7. If you want to remap priorities, then enter the new priority value under one of these priority elements.  Example: suppose you want to remap priority 5 to priority 7, then enter 7 as value of the p5 element.

Element	Description
destinationIntf	Use this element to enter the name of the (physical) destination interface which carries the VLAN when it has been switched. Default:<empty> Range: 0 … 24 characters The destination interface can also be a bridge group, in that case just enter the name of the bridge group.
destinationVlan	Use this element to enter the VLAN ID of the VLAN when it has been switched. Default:1 Range: 0 … 4094 Entering 0 as VLAN ID strips the VLAN tag of the Ethernet frame. Refer to Stripping the VLAN tag for more information.
destinationPMap	Use this element to, if desired, remap the VLAN priorities. Since the switching is bidirectional, you can remap priorities for both directions (i.e. both at the “source” and “destination” interface). Default:- Range: structure, see below Refer to the sourcePMap element for more information on this structure.

Important remarks

- Note that one row in the vlanSwitching table represents a bidirectional connection. I.e. data is switched from source to destination and vice versa.
- Also note that only point-to-point connections are possible. Point-to-multipoint connections are not possible. In other words, a certain VLAN may only appear once in the vlanSwitching table.

13.13.2 Bridge access list configuration attributes

This section describes the following configuration attributes:

- telindus24xx/bridge/accessList[ ]/macAddress on page 455

This object is not present in the containment tree by default. If you want to use the feature associated with this object, then add the object first. Refer to 4.4 - Adding an object to the containment tree on page 56.

telindus24xx/bridge/accessList[ ]/macAddress

Default:<empty>
Range: table, see below

Use this attribute to filter bridged frames based on the source MAC address.

The access list is applied on the transmitted (outgoing) data of the interface. Packets coming from MAC addresses that are specified in the access list are not sent out on the interface on which the access list is applied.

13.14 Alarm in contacts configuration attributes

This section describes the following configuration attributes:

- telindus24xx/alarmContacts/<alarmConfigurationAttributes> on page 457

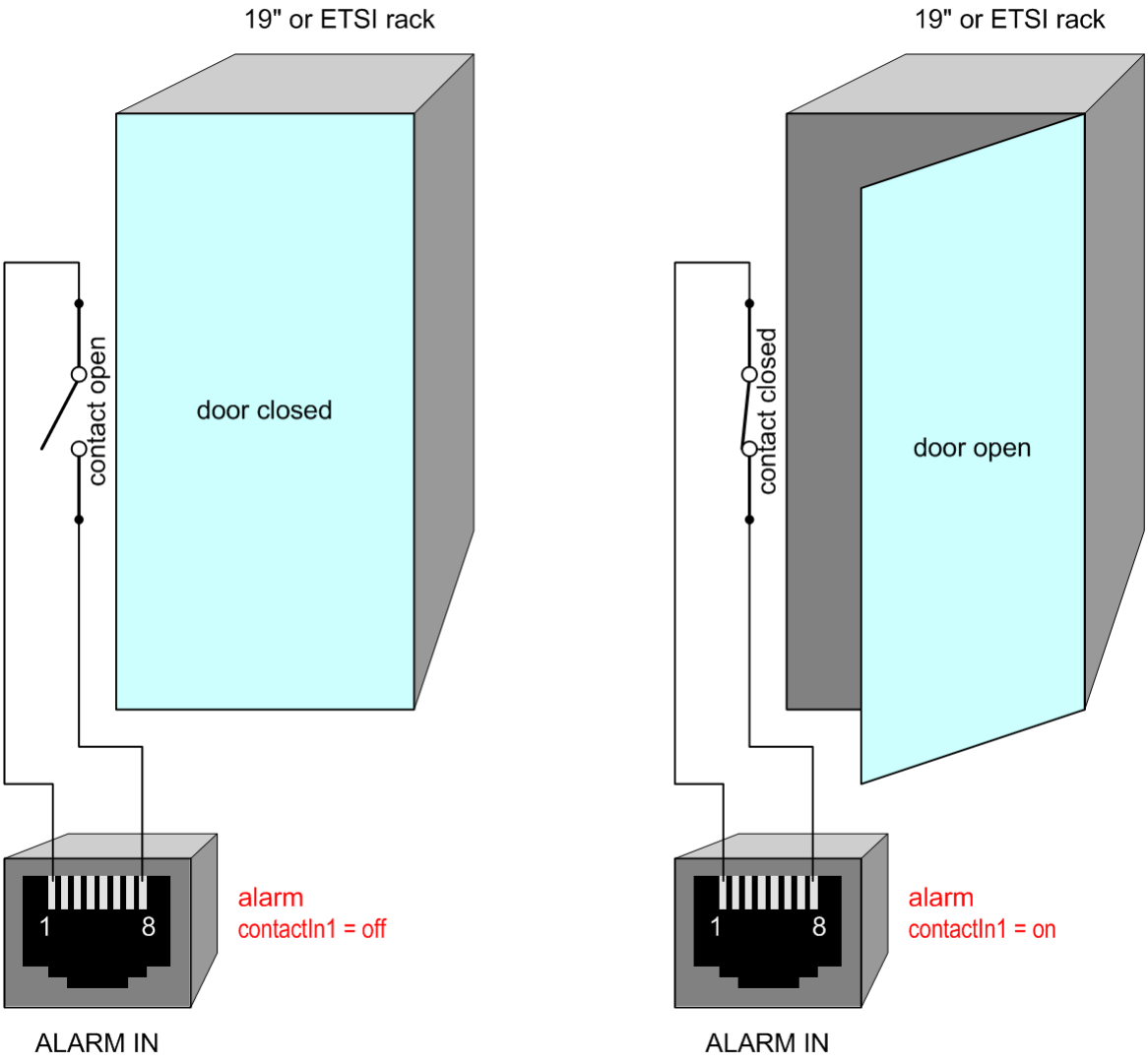
telindus24xx/alarmContacts/<alarmConfigurationAttributes>

Using the alarm in connector you can generate an internal alarm (in the Telindus 2400) in case an external alarm condition occurs.

Example

Suppose you have the following set-up:

- An 19” or ETSI rack containing, among various other devices, a Telindus 2400.
- A contact on the door of the rack. The contact is …
  - open in case the door is closed.
  - closed in case the door is open.
- The door contact is connected to pin 1 and 8 of the ALARM IN connector of the Telindus 2400.



Now the following two situations can be distinguished:

Situation	Result
rack door is closed	⇒The door contact is open. ⇒The circuit between pin 1 and 8 of the ALARM IN connector is open. ⇒The alarmContacts/contactIn1 alarm is not active.
rack door is open	⇒The door contact is closed. ⇒The circuit between pin 1 and 8 of the ALARM IN connector is closed. ⇒The alarmContacts/contactIn1 alarm is active. If the alarm is unmasked, it is sent to the central management system.

For more information on …

- the alarm in connector, refer to …
  - 2.6 - Connecting the Telindus 2400 on page 25.
  - 20.5 - Alarm in connector specifications on page 696.
- the alarm configuration attributes alarmMask, alarmLevel, alarmContactHighMask and alarmContactLowMask and on the alarms in general, refer to 16.2 - Introducing the alarm attributes on page 645.
- the alarms of the alarmContacts object, refer to 16.10 - Alarm in contacts alarms on page 663.

13.15 SNMP configuration attributes

This section describes the following configuration attributes:

- telindus24xx/snmp/trapDestinations on page 460
- telindus24xx/snmp/mib2Traps on page 460

telindus24xx/snmp/trapDestinations

Default:<empty>
Range: table, see below

Use this attribute to define to which IP address the SNMP traps have to be sent.

The Telindus 2400 translates all alarm status changes into SNMP traps. These traps can then be sent to a management system. To enable this, configure in the trapDestinations table the IP addresses to which the traps have to be sent. If the trapDestinations table is empty then no traps are sent.

The trapDestinations table contains the following elements:

Element	Description
address	Use this element to set the IP address of the management station to which the SNMP trap messages have to be sent. Default:0.0.0.0 Range: up to 255.255.255.255
community	Use this element to set the community string which is included in the SNMP traps that are sent to the management station. It is used as a password in the SNMP communication. Give it the same value as on your SNMP management station. Default:public Range: 0 … 20 characters

telindus24xx/snmp/mib2Traps

Default:off
Range: on / off

Use this attribute to enable (on) or disable (off) the sending of SNMP traps as MIB2 traps.

If you want to send the SNMP traps as MIB2 traps, proceed as follows:

Step	Action
1	Select the snmp/trapDestinations attribute. Add an entry to this table for each network management station that should receive SNMP traps. Refer to telindus24xx/snmp/trapDestinations on page 460.
2	Configure the mib2Traps attribute: **Value** / **Description** on: The alarms coldBoot, warmBoot and linkDown are sent as MIB2 traps instead of enterprise specific (private) MIB traps. off: All alarms are sent as enterprise specific (private) MIB traps.
3	Set for each object of the Telindus 2400: • the alarms that you want to send using the attribute alarmMask. • the importance of each alarm using the attribute alarmLevel. By default only the most important alarms are enabled.

13.16 Management configuration attributes

This section describes the following configuration attributes:

- telindus24xx/management/ctrlPortProtocol on page 462
- telindus24xx/management/sysLog on page 462
- telindus24xx/management/timeServer on page 464
- telindus24xx/management/timeZone on page 464
- telindus24xx/management/cms2Address on page 465
- telindus24xx/management/accessList on page 466
- telindus24xx/management/snmp on page 467
- telindus24xx/management/telnet on page 467
- telindus24xx/management/tftp on page 467
- telindus24xx/management/ftp on page 467
- telindus24xx/management/consoleNoTrafficTimeOut on page 467
- telindus24xx/management/alarmFilter on page 468
- telindus24xx/management/timedStatsAvailability on page 468
- telindus24xx/management/atwinGraphics on page 469
- telindus24xx/management/loopback/ipAddress on page 471
- telindus24xx/management/loopback/ipNetMask on page 471

telindus24xx/management/ctrlPortProtocol

Default:console
Range: enumerated, see below

Use this attribute to set the function of the control connector.

The ctrlPortProtocol attribute has the following values:

Value	Description
management	Select this value if you want to connect the control connector of the Telindus 2400 to … • a management concentrator for management purposes. • the control connector of another Telindus device using a crossed cable (i.e. they are connected back-to-back) in order to create an extended management link. Refer to What is relative and absolute addressing? on page 465 for more information on extended management links. When connecting the control connector of the Telindus 2400 to a COM port of your computer, you can still open a TMA session on the Telindus 2400. You can however not open a CLI or ATWIN session.
console	Select this value if you want to connect the control connector of the Telindus 2400 to a COM port of your computer in order to manage the Telindus 2400 using TMA, CLI, ATWIN, etc.

telindus24xx/management/sysLog

Default:-
Range: structure, see below

Use this attribute to configure the sending of syslog messages.

The sysLog structure contains the following elements:

Element	Description
separator	Use this element to specify the separator character in the syslog messages. Refer to What is syslog? on page 463 for more information on the syslog messages. Default:; Range: 1 character
destinations	Use this element to enter the IP address(es) of the syslog server(s). Up to 3 addresses can be entered. Default:<empty> Range: table, see below As soon a valid syslog server address is entered, a syslog message is sent to this server for each (unmasked) alarm that occurs. If multiple syslog server addresses are sent, then the syslog messages are sent to all servers. The syslog messages are not sent in case the interface or the route through which they have to be sent is down. In this case, the syslog messages are kept in a history list (maximum 31 messages). These pending messages are sent as soon as the interface and/or route comes up again.

What is syslog?

The syslog protocol (RFC 3164) is used for the transmission of event notification messages across networks.

A syslog message is sent on UDP port 514. It has the following format:

`"<facility*8+severity> date hostname message"`

where …

- the priority value is the number contained within the angle brackets, i.e. `<facility*8+severity>`.
- `facility` is a part of the priority value: `facility = 23 * 8 = 184`
  In this case no facility has been explicitly assigned and therefore a "local use" facility is used (numerical code value 23).
- `severity` is a part of the priority value: `severity = 6 - <alarmLevel of the alarm>`
  The severity only ranges from 0 up to 6. So in case the alarm level of an alarm is bigger than 6, the severity is limited to 0.
- `date` is the date the syslog message was generated: `Mmm dd hh:mm:ss` (e.g. `Jan 01 12:45:55`).
- `hostname` is the IP address of the interface through which the syslog message was sent (e.g. `10.0.28.3`).
- `message` is the alarm message. It has the following format:
  `"alarm:<sysName>;<realTimeClock>;<sysUpTime>;<devSeverityLevel>;<severityLevel>;<alarmMessage>"`
  where …
  - `<sysName>` is the sysName configured in the Telindus 2400.
  - `<realTimeClock>` is the value of the real time clock at the moment the alarm was generated: `dd/mm/yy hh:mm:ss` (e.g. `25/12/02 22:45:55`).
  - `<sysUpTime>` is the system up-time of the Telindus 2400 at the moment the alarm was generated: `xxxxxd xxh xxm xxs` (e.g. `00025d 08h 45m 55s`).
  - `<devSeverityLvl>` is the device severity level: `devSeverityLvl = 6 - <totalAlarmLevel of the device>`. The device severity level only ranges from 0 up to 6. So in case the total alarm level of the Telindus 2400 is bigger than 6, the device severity level is limited to 0.
  - `<severityLvl>` is the alarm severity level: `severityLvl = 6 - <alarmLevel of the alarm>`. The alarm severity level only ranges from 0 up to 6. So in case the alarm level of an alarm is bigger than 6, the alarm severity level is limited to 0.
  - `<alarmMessage>` is the alarm itself: `path.alarmName on|off` (e.g. `telindus24xx/lanInterface.linkDown on`).
  - `;` is the separator character. If desired, you can specify another separator character. Refer to the configuration element separator on page 462.

Example:

The following gives an example of a complete syslog message. In this case, the separator is the ^ character.

```
"<189>Feb 28 16:56:15 10.0.28.2 alarm:telindus24xx^28/02/03 16:56:15^130^3^5^
telindus24xx.configChanged on"
```

telindus24xx/management/timeServer

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to enter the IP address of the SNTP time server with which the Telindus 2400 can synchronise its clock. Date and time are displayed in the status attributes telindus24xx/date and telindus24xx/time.

You can also set the time zone and the daylight saving time using the configuration attribute telindus24xx/management/timeZone on page 464.

What is SNTP?

Short for Simple Network Time Protocol, a simplified version of NTP. SNTP is used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

The Telindus 2400 can only act as an SNTP client, not as an SNTP server.

telindus24xx/management/timeZone

Default:-
Range: structure, see below

Use this attribute to set the time zone when using an SNTP time server. Refer to telindus24xx/management/timeServer on page 464.

The timeZone structure contains the following elements:

Element	Description
timeZone	Use this element to set the time zone. Default:utc+1 Range: enumerated, see below The timeZone element has the following values: utc, utc+1 up to utc+12 and utc-1 up to utc-12. **What is UTC?** UTC is the coordinated universal time, formerly known as Greenwich mean time (GMT). It is the international time standard.
daylightSaving	Use this element to set the daylight saving time. Default:europeanUnion Range: europeanUnion / none The daylightSaving element has the following values: europeanUnion and none.

telindus24xx/management/cms2Address

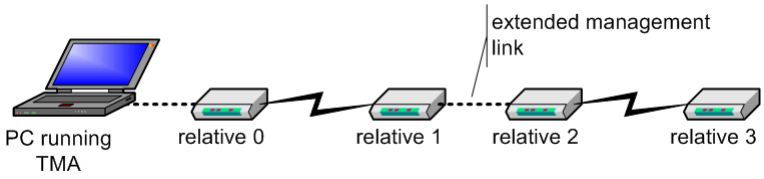
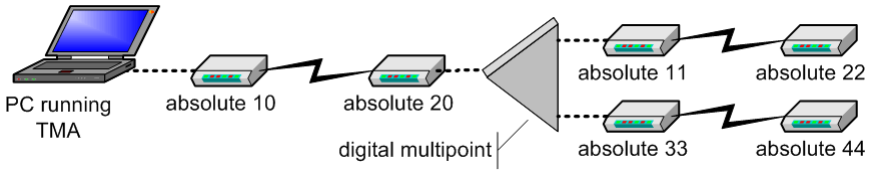
Default:0
Range: 0 … 65535

Use this attribute to assign an absolute address to the Telindus 2400.

What is relative and absolute addressing?

If you want to connect with TMA to a Telindus device, you have to specify the address of the device in the *Connect…* window. Refer to 4 - Maintaining the Telindus 2400 on page 41.

There are two different address types: relative and absolute. The following table explains the difference between these address types:

Type	Description
relative	This type of addressing is meant for a network topology where the Telindus devices are connected in-line on management level. I.e. with extended management connections between two Telindus devices. An extended management connection is realised with a crossed cable between the control connectors of two Telindus devices.  To enable relative addressing, no address has to be specified in the Telindus device. In other words, leave the cms2Address attribute at its default value, being 0.
absolute	This type of addressing is meant for a network topology where the Telindus devices are not connected in-line on management level. I.e. when there is a digital multipoint device present (e.g. an Orchid DM).  To enable absolute addressing, an address has to be specified in the Telindus device. Do this using the cms2Address attribute. The absolute addressing range goes from 1 up to 65535.

telindus24xx/management/accessList

Default:<empty>
Range: table, see below

Use this attribute to control the access from certain hosts or networks.

The access list filters incoming traffic, based on the source IP address. You can specify multiple entries within the access list. When more than one entry applies to the same packet, then only the most specific one is taken in consideration. I.e. the entry covering the smallest range. If not one entry matches, then the packet is dropped. If the access list is empty, then all packets are forwarded.

The accessList table contains the following elements:

Element	Description
sourceAddress	Use this element to set the IP source address of the packet. The address may be a (sub)network address. Default:0.0.0.0 Range: up to 255.255.255.255
mask	Use this element to set the IP subnet mask for the sourceAddress. By combining an IP address with a mask you can uniquely identify a range of addresses. Default:255.255.255.255 Range: up to 255.255.255.255
action	Use this element to set the action when a packet arrives with a source IP address that falls within the specified address range. Default:deny Range: enumerated, see below The possible actions are:

Value	Description
deny	The packet is dropped.
allow	The packet is forwarded.

If you specify one entry or multiple entries for which the action is set to deny, then also specify at least one entry for which the action is set to allow. Else all packets are dropped!

Example 1

This example shows an access list that only allows traffic from subnet 192.168.48.0, except for packets from station 192.168.48.10.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	allow
2	192.168.48.10	255.255.255.255	deny

Example 2

The next example shows an access list that allows all traffic, except the traffic from subnet 192.168.48.0. The second entry is the rule to add if you want all packets that do not match the previous entries to be allowed.

accessList

	sourceAddress	mask	action
1	192.168.48.0	255.255.255.0	deny
2	0.0.0.0	0.0.0.0	allow

telindus24xx/management/snmp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enabled) or discard (disabled) SNMP requests.

telindus24xx/management/telnet

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enabled) or discard (disabled) Telnet sessions.

Use this attribute also to accept (enabled) or discard (disabled) HTTP (Web Interface) sessions.

telindus24xx/management/tftp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enabled) or discard (disabled) TFTP sessions.

telindus24xx/management/ftp

Default:enabled
Range: enabled / disabled

Use this attribute to accept (enabled) or discard (disabled) FTP sessions.

telindus24xx/management/consoleNoTrafficTimeOut

Default:00000d 00h 30m 00s
Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

Use this attribute to set the time-out period after which a management session is closed when there is no user interaction.

The purpose of such a timer is to protect the Telindus 2400 against unauthorised access in case the last user did not close his session.

telindus24xx/management/alarmFilter

Default:0
Range: 0 … 50000

Use this attribute to selectively ignore alarms in TMA Element Management or TMA for HP OpenView if these alarms are below a certain level.

The filter number that you define using the alarmFilter attribute, has to correspond with a filter that you have to define in the Element Manager of TMA Element Management or TMA for HP OpenView. In the Element Manager, it is possible to specify a minimum alarm level that is needed before alarms are logged. This can be specified for each filter number.

Refer to manuals of TMA Element Management (PDF/CHM) or TMA for HP OpenView (PDF) for more information on alarm filtering in these applications.

telindus24xx/management/timedStatsAvailability

Default:basic
Range: enumerated, see below

Use this attribute to determine whether the nested tables in the timed performance statistics (i.e. 2 hour, 24 hour and 7 days performance statistics) are visible or not.

The timedStatsAvailability attribute has the following values:

Value	Description
none	Only the “first level” timed performance statistics are available. In other words, the nested tables (i.e. a table in a table) in the timed performance statistics are not displayed.
basic	The full performance statistics are available on the physical interfaces only (e.g. the LAN interface, etc.). Not on the logical interfaces (e.g. a PVC, a VLAN, etc.).
full	The full performance statistics are available on both the physical (e.g. the LAN interface, etc.) and logical (e.g. a PVC, a VLAN, etc.) interfaces If you have a lot of PVCs this may require quite some memory space and processing power.

telindus24xx/management/atwinGraphics

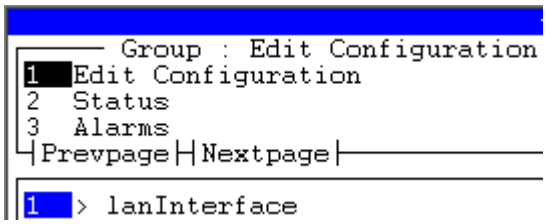
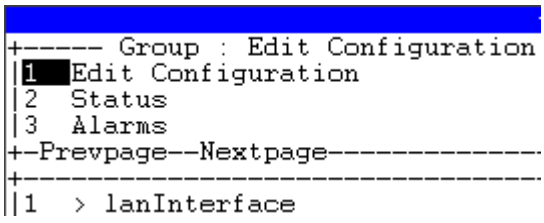
Default:enabled
Range: enabled / disabled

Use this attribute to enable or disable the graphical symbols in the ATWIN user interface.

One of the tools that allows you to manage the Telindus 2400 is ATWIN (refer to 1.6 - Maintenance and management tools on page 15). ATWIN is a basic, menu-driven user interface. You can start it using a terminal (emulation program) on the control port or using Telnet on an IP interface (e.g. the LAN interface) and by typing `atwin` at the command prompt (refer to the Maintenance tools manual (PDF) for more information).

By default, ATWIN uses graphical symbols to draw the borders of the “windows”. In some cases however, these graphical symbols are displayed incorrectly. In that case you can choose to disable the graphical symbols. By doing so, the window borders are drawn using + and - signs.

The atwinGraphics attribute has the following values:

Value	Description
enabled	The ATWIN window borders are drawn using graphical symbols. 
disabled	The ATWIN window borders are drawn using + and - signs. 

13.17 Loopback configuration attributes

This section describes the following configuration attributes:

- telindus24xx/management/loopback/ipAddress on page 471
- telindus24xx/management/loopback/ipNetMask on page 471

telindus24xx/management/loopback/ipAddress

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to assign an IP address to the loop-back interface.

The loop-back interface is a software interface which can be used for management purposes. This interface is always up, regardless of the state of the physical interfaces. This means the router will always respond to ICMP echo requests sent to this address. In every other respect the loop-back address behaves the same as an IP address of a physical interface.

If the loop-back address is used and RIP is active, then a host route to the loop-back address is included in the RIP updates.

telindus24xx/management/loopback/ipNetMask

Default:0.0.0.0
Range: up to 255.255.255.255

Use this attribute to assign an IP netmask to the loop-back interface.

Also see telindus24xx/management/loopback/ipAddress on page 471.

14 Status attributes

This chapter discusses the status attributes of the Telindus 2400. The following gives an overview of this chapter:

- 14.1 - Status attribute overview on page 474
- 14.2 - General status attributes on page 481
- 14.3 - LAN interface status attributes on page 486
- 14.4 - Cascading status attributes on page 494
- 14.5 - 4 port Ethernet interface status attributes on page 496
- 14.6 - 6E1 interface status attributes on page 497
- 14.7 - E3/T3 interface status attributes on page 502
- 14.8 - IMA group status attributes on page 509
- 14.9 - xDSL interface status attributes on page 515
- 14.10 - ATM status attributes on page 535
- 14.11 - Profile status attributes on page 542
- 14.12 - Router status attributes on page 544
- 14.13 - Bridge group status attributes on page 562
- 14.14 - Management status attributes on page 569
- 14.15 - Loopback status attributes on page 571
- 14.16 - File system status attributes on page 573
- 14.17 - Operating system status attributes on page 576

14.1 Status attribute overview

Refer to 4.3 - The objects in the Telindus 2400 containment tree on page 52 to find out which objects are present by default, which ones you can add yourself and which ones are added automatically.

> telindus24xx
- sysDescr
- sysObjectID
- sysUpTime
- sysServices
- flash1Version
- flash2Version
- activeFlash
- flashVersions
- bootVersion
- loaderVersion
- messages
- deviceId
- configurationSaving
- fan
- masterClock
- stationClockFreq
- ifModuleClockFreq
- date
- time
- day
- Action: Set Date
- Action: Set Time

>> lanInterface
- ifDescr
- ifType
- ifOperStatus
- ifLastChange
- ifSpeed
- ifMtu
- ip
- macAddress
- arpCache
- bridging
- adapter
- vlan
- ipAdEntBcastAddr
- ipAdEntReasmMaxSize
- Action: clearArpCache

>>> atm
- cascadeTable

>> 4pEth

ifDescr
ifType
ifOperStatus
ifLastChange
ifSpeed
ifMtu
ip
macAddress
arpCache
bridging
vlan
ipAdEntBcastAddr
ipAdEntReasmMaxSize
deviceId
Action: clearArpCache

>> hexE1

ifClocking
deviceId

>>> e1[E1_x]

ifDescr
ifType
ifOperStatus
ifSpeed
los
ais
lfa
rai
tcCellDeliniation

>> e3T3

deviceId

>>> e3T3[E3T3_x]

ifDescr
ifType
ifOperStatus
ifSpeed
los
ais
lfa
rai

>>>> atm

atmSync
pvc
vp

>> bundle

>>> imaGroup[ ]

pvc
neState
feState
failure
numActRxLinks
numActTxLinks
neTxClockMode
feTxClockMode
members

>> dslInterfaces[1]

>>> interface[dsl_x]

ifIndex
ifDescr
ifType
ifOperStatus

>>>> line

ifDescr
ifType
ifOperStatus
ifSpeed
region
numDiscoveredRepeaters
eocAlarmThresholds
eocStatus

>>>>> linePair

ifAdminStatus
ifOperStatus
ifSpeed
status
timeSinceLastRetrain
lineAttenuation
noiseMargin
actualBitRate
physLinePair

1. SHDSL line status attributes. Telindus 2400 SHDSL models only (2421, 2422, 2423).

>>>> repeater
- vendorId
- vendorModel
- vendorSerial
- vendorSoftVersion
- eocSoftVersion
- shdslVersion
- eocStatus
- eocAlarmThresholds

>>>>> linePair
- lineAttenuation
- noiseMargin
- Action: loopbackActivation

>>>> end
- vendorId
- vendorModel
- vendorSerial
- vendorSoftVersion
- eocSoftVersion
- shdslVersion
- eocStatus
- eocAlarmThresholds

>>>>> linePair
- lineAttenuation
- noiseMargin

>>>> atm
- atmSync
- pvc
- vp

>> dslInterfaces[2]

>>> interface[dsl_x]
- ifIndex
- ifDescr
- ifType
- ifOperStatus

2. ADSL line status attributes. Telindus 2400 ADSL models only (2401, 2402, 2403).

>>>> line

ifDescr
ifType
ifOperStatus
ifUsSpeed
ifDsSpeed
standard

>>>>> linePair

status
progress
timeSinceLastRetrain
lineAttenuation
noiseMargin
transmitPower
usInterleaveDelay
dsInterleaveDelay

>>>> end

vendorId
vendorRevision
vendorSerial

>>>>> linePair

lineAttenuation
noiseMargin
transmitPower

>>>> atm

atmSync
pvc
vp

>> profiles

>>> xdsl

>>>> shdsl_default[3]

profileUsers

>>>> adsl_default[4]

profileUsers

3. Telindus 2400 SHDSL models only (2421, 2422, 2423).
4. Telindus 2400 ADSL models only (2401, 2402, 2403).

>>> atm

>>>> pvc_default
profileUsers

>>> forwardingMode

>>>> routing_default
profileUsers

>>>> bridging_default
profileUsers

>>> lineConfiguration

>>>> shdslAtm_default[5]
profileUsers

>>>> adslAtm_default[6]
profileUsers

>> ip

>>> router
routingTable
igmpTable
dhcpBinding
dhcpStatistics
dhcpRelayInfo
radius
dns
addrPools

>>>> defaultNat
addresses

>>>> tunnels
l2tpTunnels
ipsecL2tpTunnels

5. Telindus 2400 SHDSL models only (2421, 2422, 2423).
6. Telindus 2400 ADSL models only (2401, 2402, 2403).

>> bridge

>>> bridgeGroup
- ifDescr
- ifType
- ifOperStatus
- ifMtu
- ip
- macAddress
- arpCache
- bridgeCache
- bridging
- spanningTree
- Action: clearArpCache
- Action: clearBridgeCache

>> management
- cms2Address
- timeServer
- alarmLog

>>> loopback
- ifDescr
- ifType
- ifOperStatus
- ifMtu
- ipAddress
- mask

>> fileSystem
- fileList
- freeSpace
- status
- corruptBlocks
- Action: Delete File
- Action: Rename File

>> operatingSystem
- taskInfo

14.2 General status attributes

This section describes the following status attributes:

- telindus24xx/sysDescr on page 482
- telindus24xx/sysObjectID on page 482
- telindus24xx/sysUpTime on page 482
- telindus24xx/sysServices on page 482
- telindus24xx/flash1Version on page 482
- telindus24xx/flash2Version on page 482
- telindus24xx/activeFlash on page 483
- telindus24xx/flashVersions on page 483
- telindus24xx/bootVersion on page 483
- telindus24xx/loaderVersion on page 483
- telindus24xx/messages on page 483
- telindus24xx/deviceId on page 484
- telindus24xx/configurationSaving on page 484
- telindus24xx/fan on page 484
- telindus24xx/masterClock on page 484
- telindus24xx/stationClockFreq on page 484
- telindus24xx/ifModuleClockFreq on page 484
- telindus24xx/date on page 485
- telindus24xx/time on page 485
- telindus24xx/day on page 485
- telindus24xx/Set Date on page 485
- telindus24xx/Set Time on page 485

telindus24xx/sysDescr

This attribute displays a textual description of the device.

Example: Telindus 2400 Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Telindus 2400 is the device name.
- Txxxx/xxxxx is the application software code and version.
- 01/01/00 12:00 is the application software release date and time.

telindus24xx/sysObjectID

This attribute displays the identification string.

telindus24xx/sysUpTime

This attribute displays the elapsed time since the last power-on or cold boot of the Telindus 2400.

telindus24xx/sysServices

This attribute displays the service identification.

telindus24xx/flash1Version

This attribute displays the code and version of the application software stored as CONTROL1.

Example: Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Txxxx is the application software code for this device.
- /xxxxx is the application software version.
- 01/01/00 is the application software release date.
- 12:00 is the application software release time.

telindus24xx/flash2Version

This attribute displays the code and version of the application software stored as CONTROL2.

Example: Txxxx/xxxxx 01/01/00 12:00

In this example the following parameters are visible:

- Txxxx is the application software code for this device.
- /xxxxx is the application software version.
- 01/01/00 is the application software release date.
- 12:00 is the application software release time.

telindus24xx/activeFlash

This attribute displays which application software is currently active. Possible values are:

Value	Description
flash1	The application software CONTROL1 is active.
flash2	The application software CONTROL2 is active.

telindus24xx/flashVersions

This attribute displays how many application software versions can be stored in the file system.

telindus24xx/bootVersion

This attribute displays the code, version, release date and time of the boot software currently used in the Telindus 2400.

telindus24xx/loaderVersion

This attribute displays the code, version, release date and time of the loader software currently used in the Telindus 2400.

telindus24xx/messages

This attribute displays informative and error messages, e.g. Reconfigured, Cold Boot, … The messages table displays maximum 20 messages.

If you open a TMA session on the Telindus 2400 over IP, i.e. not through the control port, then the messages are also sent to the control port. This means that if you open a terminal emulation session on the control port, you can monitor these messages. If you hit the ENTER key, the messages stop and you get the (CLI) password prompt.

telindus24xx/deviceId

This attribute displays a unique code. This code is programmed into the Telindus 2400 before it leaves the factory. You can use this code for inventory purposes.

telindus24xx/configurationSaving

This attribute indicates when the Telindus 2400 is writing its (new) configuration to the flash memory. Possible values are:

Value	Description
busy	The Telindus 2400 is busy writing its configuration to the flash memory. During this state, do not power-down or reboot the Telindus 2400 else the new configuration will be lost.
done	The Telindus 2400 has finished writing its configuration to the flash memory.

telindus24xx/fan

This attribute displays the status of the fan. The fan should be running to avoid overheating.

telindus24xx/masterClock

This attribute displays the master clocking mode as you configured it.

telindus24xx/stationClockFreq

This attribute displays the frequency of the station clock (if present).

telindus24xx/ifModuleClockFreq

This attribute displays the frequency of the TIM interface clock (if present).

telindus24xx/date

This attribute displays the current date in the format dd/mm/yy (e.g. 01/01/00).

telindus24xx/time

This attribute displays the current time in the format hh:mm:ss (e.g. 12:30:45).

telindus24xx/day

This attribute displays the current day of the week (e.g. monday).

telindus24xx/Set Date

Use this action to set the current date. Enter the date as argument value in the format dd/mm/yy (e.g. 01/01/00). Then execute the action.

telindus24xx/Set Time

Use this action to set the current time. Enter the time as argument value in the format hh:mm:ss (e.g. 12:30:45). Then execute the action.

14.3 LAN interface status attributes

This section describes the following status attributes:

- telindus24xx/lanInterface/ifDescr on page 487
- telindus24xx/lanInterface/ifType on page 487
- telindus24xx/lanInterface/ifOperStatus on page 487
- telindus24xx/lanInterface/ifLastChange on page 487
- telindus24xx/lanInterface/ifSpeed on page 487
- telindus24xx/lanInterface/ifMtu on page 487
- telindus24xx/lanInterface/ip on page 488
- telindus24xx/lanInterface/macAddress on page 488
- telindus24xx/lanInterface/arpCache on page 489
- telindus24xx/lanInterface/bridging on page 490
- telindus24xx/lanInterface/adapter on page 492
- telindus24xx/lanInterface/vlan on page 492
- telindus24xx/lanInterface/ipAdEntBcastAddr on page 493
- telindus24xx/lanInterface/ipAdEntReasmMaxSize on page 493

This section describes the following actions:

- telindus24xx/lanInterface/clearArpCache on page 493

telindus24xx/lanInterface/ifDescr

This attribute displays the interface description.

telindus24xx/lanInterface/ifType

This attribute displays the interface type.

telindus24xx/lanInterface/ifOperStatus

This attribute displays the current operational status of the interface.

telindus24xx/lanInterface/ifLastChange

This attribute shows the system-up time on the moment the interface entered its current operational state. I.e. the moment the value of the ifOperStatus status attribute changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status attribute.

telindus24xx/lanInterface/ifSpeed

This attribute displays the interface speed in bits per second (bps).

telindus24xx/lanInterface/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

telindus24xx/lanInterface/ip

This attribute displays the IP information of the interface.

The ip structure contains the following elements:

Element	Description
status	This is the current operational status of the IP layer (layer 3).
address	This is the IP address of the interface. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the interface. It is either configured or retrieved automatically.
secondaryIp	This table displays the secondary IP addresses as you configured them. The secondaryIp table contains the elements address and netMask.

telindus24xx/lanInterface/macAddress

This attribute displays the MAC address of the LAN interface.

The LAN interface has been allocated a fixed Ethernet address, also called MAC (Medium Access Control) address. The MAC address is globally unique and can not be modified. It is a 6 byte code, represented in hexadecimal format. Each byte in the code is separated by a colon.

Refer to What is the ARP cache? on page 314 for more information on the MAC addresses.

telindus24xx/lanInterface/arpCache

This attribute displays all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface. Refer to What is the ARP cache? on page 314 for more information.

The arpCache table contains the following elements:

Element	Description
macAddress	This is the MAC address.
ipAddress	This is the associated IP address.
type	This is the ARP cache entry type. Possible values are: **Value** / **Description** dynamic: The MAC - IP address pair is retrieved from an ARP request or reply message. static: The MAC - IP address pair is configured. There is only one static entry, i.e. the Telindus 2400 its own IP and MAC address.
timeOut	This is the time the entry will remain in the ARP cache. For the static entry, this value is 0.

Example

The following figure shows part of an ARP cache table as an example:

arpCache

	macAddress	ipAddress	type	timeout
1	00:20:AF:BD:A7:9B	194.7.48.84	dynamic	00000d 01h 12m 17s
2	00:00:0C:40:29:B1	194.7.48.37	dynamic	00000d 01h 59m 55s
3	00:50:8B:2E:3B:94	194.7.48.163	dynamic	00000d 01h 59m 56s
4	00:10:4B:B1:34:1C	10.0.8.128	dynamic	00000d 01h 58m 19s
5	00:50:04:40:8B:C2	194.7.48.148	dynamic	00000d 01h 59m 56s
6	00:08:C7:09:40:10	194.7.48.10	dynamic	00000d 01h 59m 02s
7	00:10:5A:AD:32:56	194.7.48.185	dynamic	00000d 01h 58m 11s
8	00:10:5A:FB:BA:8E	10.0.8.154	dynamic	00000d 01h 55m 06s
9	00:20:AF:F1:EE:3A	10.0.8.180	dynamic	00000d 01h 56m 48s
10	00:10:83:27:17:97	194.7.48.60	dynamic	00000d 01h 59m 31s

telindus24xx/lanInterface/bridging

This attribute displays the bridging status of the interface.

The bridging structure contains the following elements:

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>state</td><td>This displays the current state of the port. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>disabled *</td><td>The port is not in use because of a management action.</td></tr>
<tr><td>blocking</td><td>The port does not participate in frame forwarding.</td></tr>
<tr><td>listening</td><td>The port prepares to participate in frame forwarding, but it does not update its MAC address database (also called bridge cache).</td></tr>
<tr><td>learning</td><td>The port prepares to participate in frame forwarding, and it learns the present MAC addresses.</td></tr>
<tr><td>forwarding *</td><td>The port participates in frame forwarding.</td></tr>
</table>
* These are the only possible port states for a bridge that is not running the Spanning Tree protocol (IEEE p802.1D).

Refer to 10.1.5 - The Spanning Tree bridge port states on page 229 for more information on port states.[1]</td></tr>
<tr><td>subState[1]</td><td>This gives additional information on the port state. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>root</td><td>This is the port through which the root bridge can be reached. Consequently, the root bridge itself does not have a root port. All other bridges must have a root port.</td></tr>
<tr><td>designated</td><td>This is the designated port for this (virtual) LAN. All ports of the root bridge are designated ports.</td></tr>
<tr><td>alternate</td><td>This port is not active. Either because of a management action, or through protocol intervention.</td></tr>
</table>
</td></tr>
</table>

Element	Description
designatedPriority[1]	Together, these two elements form a unique bridge identifier. Depending whether the current port is a designated port or not, these two elements display the unique bridge identifier of … • the bridge to which this port belongs, in case of a designated port. • the bridge believed to be the designated bridge for the LAN that is currently connected to this port, in all other cases. This bridge identifier is used … • together with the designatedPortPriority and designatedPortId attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port. • to test the value of the bridge identifier parameter conveyed in received Configuration BPDUs.
designatedMac[1]	
designatedPort-Priority[1]	Together, these two elements form a unique port identifier. They display the unique port identifier of the bridge port through which the designated bridge transmits the configuration message information stored by this port. This port identifier is used … • together with the designatedPriority and designatedMac attributes to determine whether this port should be the designated port for the LAN that is currently connected to this port. • by the management system to determine the topology of the bridged LAN.
designatedPortId[1]	
topologyChangeAck[1]	This displays the value of the Topology Change Acknowledgement flag in the next Configuration BPDU that will be transmitted on this port. This element is used to assess the need to set the Topology Change Acknowledgement flag in response to a received Topology Change Notification BPDU.
configuration-Pending[1]	This is used to determine whether a Configuration BPDU should be transmitted on this port after expiry of the hold timer. This avoids that Configuration BPDUs are transmitted too often, although ensuring that up-to-date information is transmitted.

1. Only relevant when the bridge uses the Spanning Tree Protocol.

telindus24xx/lanInterface/adapter

This attribute displays the Ethernet mode of the LAN interface as you configured it.

The adapter structure contains the following elements:

Element	Description
speed	This is the Ethernet speed. Possible values are: 10 and 100.
duplex	This is the Ethernet duplex mode. Possible values are: halfDuplex and fullDuplex.

telindus24xx/lanInterface/vlan

This attribute displays the status of the VLAN(s) on this interface.

The vlan table contains the following elements:

Element	Description
name	This is the name of the VLAN as you configured it. If you did not configure a name, then this element displays: <LAN interface name> “vlan” <VLAN ID>. E.g. lan vlan 2
ifOperStatus	This is the current operational status of the VLAN.
ifLastChange	This is the system-up time on the moment the VLAN entered its current operational state. I.e. the moment the value of the ifOperStatus element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange element.
ip	This displays the IP address and subnet mask of the VLAN.
bridging	This displays the bridging information of the VLAN. Refer to telindus24xx/lanInterface/bridging on page 490 for a detailed description of the bridging structure.
vlan	This displays the specific VLAN related status information. The vlan structure contains the following elements:

Element	Description
identifier	This element displays the VLAN identifier.
arpCache	This element displays all the MAC address - IP address pairs from ARP requests and replies received on the VLAN. Refer to telindus24xx/lanInterface/arpCache on page 489 for a detailed description of the arpCache table.

telindus24xx/lanInterface/ipAdEntBcastAddr

This attribute displays the value of the least-significant bit in the IP broadcast address. This address is used for sending packets on the interface which is associated with the IP address of this entry. The value applies to the general broadcast, the subnet and network broadcasts.

telindus24xx/lanInterface/ipAdEntReasmMaxSize

This attribute displays the size of the largest IP packet which this entity can re-assemble from incoming IP fragmented packets received on this interface.

telindus24xx/lanInterface/clearArpCache

If you execute this action, the ARP cache table is cleared.

14.4 Cascading status attributes

This section describes the following status attributes:

• telindus24xx/lanInterface/atm/cascadeTable on page 495

telindus24xx/lanInterface/atm/cascadeTable

This attribute displays some ATM switch cascading information.

The cascadeTable contains the following elements:

Element	Description
name	This element displays the name as you configured it in the configuration attribute cascadeTable. Refer to telindus24xx/lanInterface/atm/cascadeTable on page 321.
ip	This element displays the LAN IP address of the ATM switch you cascade to.
mac	This element displays the LAN MAC address of the ATM switch you cascade to.

14.5 4 port Ethernet interface status attributes

The status attributes of the 4 port Ethernet interface are the same as those of the LAN interface. Refer to 14.3 - LAN interface status attributes on page 486.

However, there are two exceptions:

- The status attribute adapter is present on the LAN interface, but not on the 4 port Ethernet interface. On the LAN interface this attribute shows you the Ethernet mode how you configured it using the configuration attribute adapter. On the 4 port Ethernet interface the configuration attribute adapter is not present and therefore also the status attribute adapter is not present.
- The status attribute deviceId is present on the 4 port Ethernet interface, but not on the LAN interface. On the 4 port Ethernet interface this attribute displays a unique code. This code is programmed into the 4 port Ethernet interface before it leaves the factory. You can use this code for inventory purposes.

14.6 6E1 interface status attributes

This section discusses the status attributes of the 6E1 interface. First it describes the status attributes of the interface as a whole, then of the separate E1 interfaces.

The following gives an overview of this section:

- 14.6.1 - General 6E1 interface status attributes on page 498
- 14.6.2 - Specific E1 interface status attributes on page 500

14.6.1 General 6E1 interface status attributes

This section describes the following status attributes:

- telindus24xx/hexE1/ifClocking on page 499
- telindus24xx/hexE1/deviceId on page 499

telindus24xx/hexE1/ifClocking

This attribute displays the 6E1 interface clocking mode as you configured it.

telindus24xx/hexE1/deviceId

This attribute displays a unique code. This code is programmed into the 6E1 interface before it leaves the factory. You can use this code for inventory purposes.

14.6.2 Specific E1 interface status attributes

This section describes the following status attributes:

- telindus24xx/hexE1/e1[E1_x]/ifDescr on page 501
- telindus24xx/hexE1/e1[E1_x]/ifType on page 501
- telindus24xx/hexE1/e1[E1_x]/ifOperStatus on page 501
- telindus24xx/hexE1/e1[E1_x]/ifSpeed on page 501
- telindus24xx/hexE1/e1[E1_x]/los on page 501
- telindus24xx/hexE1/e1[E1_x]/lfa on page 501
- telindus24xx/hexE1/e1[E1_x]/ais on page 501
- telindus24xx/hexE1/e1[E1_x]/rai on page 501
- telindus24xx/hexE1/e1[E1_x]/tcCellDeliniation on page 501

telindus24xx/hexE1/e1[E1_x]/ifDescr

This attribute displays the interface description.

telindus24xx/hexE1/e1[E1_x]/ifType

This attribute displays the interface type.

telindus24xx/hexE1/e1[E1_x]/ifOperStatus

This attribute displays the current operational status of the interface.

telindus24xx/hexE1/e1[E1_x]/ifSpeed

This attribute displays the interface speed in bits per second (bps).

telindus24xx/hexE1/e1[E1_x]/los

This attribute displays (on / off) whether a Loss Of Signal has been detected. LOS is on when the incoming data is no longer present.

telindus24xx/hexE1/e1[E1_x]/lfa

This attribute displays (on / off) whether a Loss of Frame Alignment has been detected. LFA is on when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period.

telindus24xx/hexE1/e1[E1_x]/ais

This attribute displays (on / off) whether an Alarm Indication Signal has been detected. AIS is on when the AIS signal (also called *all ones*) is detected on the incoming data. AIS means there is an alarm occurring on the line upstream from the equipment that is connected to the G.703 interface.

telindus24xx/hexE1/e1[E1_x]/rai

This attribute displays (on / off) whether a Remote Alarm Indication signal has been detected. RAI is on when the RAI signal is detected on the incoming data. RAI means the far-end equipment has a problem with the signal it is receiving from the local equipment.

telindus24xx/hexE1/e1[E1_x]/tcCellDeliniation

This attribute displays the status of the TC (Transmission Convergence) layer. Possible values are:

Value	Description
aligned	The (ATM) cell delineation state is in the sync state. In this state, the TC is assumed to be synchronised so that other functions can be applied to the cell.
notAligned	The (ATM) cell delineation state is in the hunt or pre-sync state. When a number of good HECs (Header Error Check, i.e. ATM header CRCs) are found, the state moves to sync.

14.7 E3/T3 interface status attributes

This section discusses the status attributes of the E3/T3 interface. First it describes the general E3/T3 interface status attributes and then the specific E3/T3 interface status attributes. Finally, it explains the ATM related status attributes of the E3/T3 interface.

The following gives an overview of this section:

- 14.7.1 - General E3/T3 interface status attributes on page 503
- 14.7.2 - Specific E3/T3 interface status attributes on page 505
- 14.7.3 - ATM status attributes on the E3/T3 interface on page 507

14.7.1 General E3/T3 interface status attributes

This section describes the following status attributes:

• telindus24xx/e3T3/deviceId on page 504

telindus24xx/e3T3/deviceId

This attribute displays a unique code. This code is programmed into the E3/T3 interface before it leaves the factory. You can use this code for inventory purposes.

14.7.2 Specific E3/T3 interface status attributes

This section describes the following status attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/ifDescr on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/ifType on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/ifOperStatus on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/ifSpeed on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/los on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/lfa on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/ais on page 506
- telindus24xx/e3T3/e3T3[E3T3_x]/rai on page 506

telindus24xx/e3T3/e3T3[E3T3_x]/ifDescr

This attribute displays the interface description.

telindus24xx/e3T3/e3T3[E3T3_x]/ifType

This attribute displays the interface type.

telindus24xx/e3T3/e3T3[E3T3_x]/ifOperStatus

This attribute displays the current operational status of the interface.

telindus24xx/e3T3/e3T3[E3T3_x]/ifSpeed

This attribute displays the interface speed in bits per second (bps).

telindus24xx/e3T3/e3T3[E3T3_x]/los

This attribute displays (on / off) whether a Loss Of Signal has been detected. LOS is on when the incoming data is no longer present.

telindus24xx/e3T3/e3T3[E3T3_x]/lfa

This attribute displays (on / off) whether a Loss of Frame Alignment has been detected. LFA is on when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period.

telindus24xx/e3T3/e3T3[E3T3_x]/ais

This attribute displays (on / off) whether an Alarm Indication Signal has been detected. AIS is on when the AIS signal (also called *all ones*) is detected on the incoming data. AIS means there is an alarm occurring on the line upstream from the equipment that is connected to the G.703 interface.

telindus24xx/e3T3/e3T3[E3T3_x]/rai

This attribute displays (on / off) whether a Remote Alarm Indication signal has been detected. RAI is on when the RAI signal is detected on the incoming data. RAI means the far-end equipment has a problem with the signal it is receiving from the local equipment.

14.7.3 ATM status attributes on the E3/T3 interface

This section describes the following status attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/atm/atmSync on page 508
- telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc on page 508
- telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp on page 508

telindus24xx/e3T3/e3T3[E3T3_x]/atm/atmSync

This attribute displays the ATM synchronisation status. Possible values are: synced, notSynced.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc

This attribute gives the complete status information of all the PVCs that are present on the E3/T3 interface.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc on page 536 for a detailed description of the pvc table.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp

Whereas the pvc table gives the current operational status for each Virtual Channel, the vp table gives the current operational status of a complete Virtual Path.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp on page 541 for a detailed description of the vp table.

14.8 IMA group status attributes

This section describes the following status attributes:

- telindus24xx/bundle/imaGroup[ ]/pvc on page 510
- telindus24xx/bundle/imaGroup[ ]/neState on page 510
- telindus24xx/bundle/imaGroup[ ]/feState on page 510
- telindus24xx/bundle/imaGroup[ ]/failure on page 511
- telindus24xx/bundle/imaGroup[ ]/numActRxLinks on page 512
- telindus24xx/bundle/imaGroup[ ]/numActTxLinks on page 512
- telindus24xx/bundle/imaGroup[ ]/neTxClockMode on page 512
- telindus24xx/bundle/imaGroup[ ]/feTxClockMode on page 512
- telindus24xx/bundle/imaGroup[ ]/members on page 513

telindus24xx/bundle/imaGroup[ ]/pvc

This attribute gives the complete status information of all the PVCs that are part of the IMA group.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc on page 536 for a detailed description of the pvc table.

telindus24xx/bundle/imaGroup[ ]/neState

This attribute displays the current operational status of the near-end of the IMA group. Possible values are:

Value	Description
notConfigured	This is a group state indicating that the group does not exist yet.
startUp	This is a group state indicating that the group is waiting to see the far-end in start-up.
startUpAck	This is a group transitional state, when both groups are in startup and the far-end group parameters have been accepted.
configAbortUnsup-portedM	This is a group state indicating that the group has rejected the group parameters proposed by the far-end IMA group. The reason in this case is “unsupported IMA frame size”.
configAbortIncom-patibleSymmetry	This is a group state indicating that the group has rejected the group parameters proposed by the far-end IMA group. The reason in this case is “incompatible group symmetry” (the Telindus 2400 does not support asymmetrical operation).
configAbortInvalid-ImaVersion	This is a group state indicating that the group has rejected the group parameters proposed by the far-end IMA group. The reason in this case is “unsupported IMA version”.
configAbortOther	This is a group state indicating that the group has rejected the group parameters proposed by the far-end IMA group. The reason in this case is any other reason than configAbortUnsupportedM, configAbortIncompatibleSymmetry or configAbortInvalidImaVer-sion.
insufficientLinks	Group state indicating that the group does not have sufficient links in the active state to be in the operational state.
blocked	This is a group state indicating that the group has been inhibited.
operational	Group state indicating than the group has sufficient links in both transmit and receive directions to carry ATM layer cells.

telindus24xx/bundle/imaGroup[ ]/feState

This attribute displays the current operational status of the far-end of the IMA group. The possible values are the same as those of the neState attribute. Refer to telindus24xx/bundle/imaGroup[ ]/neState on page 510.

telindus24xx/bundle/imaGroup[ ]/failure

This attribute displays the current failure status of the IMA group (the reason why the IMA group is down). Possible values are:

Value	Description
noFailure	There is no failure. The IMA group is up.
startUpNe	The near-end does not start up.
startUpFe	The far-end does not start up.
invalidMValueNe	An unsupported IMA frame size is proposed by the near-end.
invalidMValueFe	An unsupported IMA frame size is proposed by the far-end.
failedAssymetricNe	The number of active links proposed by the near-end does not match the number of active links on the far-end.
failedAssymetricFe	The number of active links proposed by the far-end does not match the number of active links on the near-end.
insufficientLinksNe	The near-end does not have sufficient links in the active state to be in the operational state.
insufficientLinksFe	The far-end does not have sufficient links in the active state to be in the operational state.
blockedNe	The near-end has been inhibited.
blockedFe	The far-end has been inhibited.
invalidImaVerionNe	An unsupported IMA version is proposed by the near-end.
invalidImaVersionFe	An unsupported IMA version is proposed by the far-end.
otherFailure	The reason of the failure is any other reason than one stated above.

telindus24xx/bundle/imaGroup[ ]/numActRxLinks

This attribute displays the number of active, receiving links.

telindus24xx/bundle/imaGroup[ ]/numActTxLinks

This attribute displays the number of active, transmitting links.

telindus24xx/bundle/imaGroup[ ]/neTxClockMode

This attribute displays the transmit clock mode that is currently being used by the near-end. Possible values are:

Value	Description
common	This is Common Transmit Clock configuration (CTC). This is a configuration where the transmit clocks of all the physical links within the IMA group are derived from the same clock source.
independent	This is Independent Transmit Clock configuration (ITC). This is a configuration where there is a transmit clock of at least one link within the IMA group that is not derived from a clock source different from some of the other transmit links.

telindus24xx/bundle/imaGroup[ ]/feTxClockMode

This attribute displays the transmit clock mode that is currently being used by the far-end. Possible values are:

Value	Description
common	This is Common Transmit Clock configuration (CTC). This is a configuration where the transmit clocks of all the physical links within the IMA group are derived from the same clock source.
independent	This is Independent Transmit Clock configuration (ITC). This is a configuration where there is a transmit clock of at least one link within the IMA group that is not derived from a clock source different from some of the other transmit links.

telindus24xx/bundle/imaGroup[ ]/members

This attribute gives the complete status information of all the members of the IMA group.

The members table contains the following elements:

Element	Description
interface	This element displays the name of the E1 interface that is a member of the IMA group.
id	This element displays the logical ID of the link on the E1 interface that makes up the IMA bundle.
neRxState	This element displays the current status of the near-end receive side of the link. Possible values are:
neTxState	This element displays the current status of the near-end transmit side of the link. The possible values are the same as those of the neRxState element. Refer to neRxState on page 513.

Value	Description
notInGroup	This is a state indicating the link is no longer configured within an IMA group.
unusableNoGivenReason	This is a state indicating the link is not in use. In this case, no reason can be given why the link is not in use.
unusableFault	This is a state indicating the link is not in use. The reason in this case is “fault”. This means a fault has been detected either on the link or in the link protocol.
unusableMisconnected	This is a state indicating the link is not in use. The reason in this case is “misconnected”.
unusableInhibited	This is a state indicating the link is not in use. The reason in this case is “inhibited”. This means operation of the link is blocked for some locally defined application or implementation dependent reason.
unusableFailed	This is a state indicating the link is not in use. The reason in this case is “failed”. This means the link fails due to the persistence of a defined defect.
usable	This is a state indicating the link is ready to be used.
active	This is a state indicating the link is capable of passing cells from the ATM layer.
deleted	This is a state indicating the link has been removed from the IMA group.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>feRxState</td><td>This element displays the current status of the far-end receive side of the link.
The possible values are the same as those of the neRxState element. Refer to neRxState on page 513.</td></tr>
<tr><td>feTxState</td><td>This element displays the current status of the far-end transmit side of the link.
The possible values are the same as those of the neRxState element. Refer to neRxState on page 513.</td></tr>
<tr><td>neRxFailure</td><td>This element displays the current failure status of the near-end receive side of the link. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>noFailure</td><td>There is no failure. The near-end side of the link is up.</td></tr>
<tr><td>imaLinkFailure</td><td>The complete link is down.</td></tr>
<tr><td>lifFailure</td><td>A LIF (Loss of IMA Frame) defect is detected.
A LIF defect is the occurrence of persistent OIF (Out of IMA Frame) anomalies for at least 2 IMA frames.</td></tr>
<tr><td>lodsFailure</td><td>A LODS (Link Out of Delay Synchronization) defect is detected.
The LODS is a link event indicating that the link is not synchronized with the other links within the IMA group.</td></tr>
<tr><td>misConnected</td><td>This is reported when the IMA unit has determined that the receive link is not connected to the same far-end IMA unit as the other receive links in the group.</td></tr>
<tr><td>blocked</td><td>The link is blocked.</td></tr>
<tr><td>fault</td><td>A fault is detected either on the link or in the link protocol.</td></tr>
<tr><td>farEndTxLinkUnusable</td><td>The far-end transmit side of the link is unusable.</td></tr>
<tr><td>farEndRxLinkUnusable</td><td>The far-end receive side of the link is unusable.</td></tr>
</table></td></tr>
</table>

14.9 xDSL interface status attributes

This section lists the status attributes of the SHDSL and ADSL interfaces. First it lists the status attributes that apply on both the SHDSL and ADSL interfaces. Then it lists the status attributes that are specific for the SHDSL line, line pair, repeater and end device. Following this it lists the status attributes that are specific for the ADSL line, line pair and end device.

- On a Telindus 2400 ADSL model, the line, linePair and end objects are always present. The repeater object does not exist on this model.
- On a Telindus 2400 SHDSL model, the line, linePair, repeater and end objects are added dynamically:
  - The line and linePair objects only appear when the necessary profiles have been configured and applied.
  - The repeater and end objects only appear when a connection with a repeater and/or remote SHDSL device has been established successfully.

The following gives an overview of this section:

- 14.9.1 - General xDSL interface status attributes on page 516
- 14.9.2 - SHDSL line status attributes on page 519
- 14.9.3 - SHDSL line pair status attributes on page 523
- 14.9.4 - SHDSL repeater and end status attributes on page 526
- 14.9.5 - ADSL line status attributes on page 529
- 14.9.6 - ADSL line pair status attributes on page 531
- 14.9.7 - ADSL end status attributes on page 533

14.9.1 General xDSL interface status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/ifIndex on page 517
- telindus24xx/dslInterfaces/interface[dsl_x]/ifDescr on page 517
- telindus24xx/dslInterfaces/interface[dsl_x]/ifType on page 517
- telindus24xx/dslInterfaces/interface[dsl_x]/ifOperStatus on page 517

telindus24xx/dslInterfaces/interface[dsl_x]/ifIndex

This attribute displays the physical index of the xDSL interface.

telindus24xx/dslInterfaces/interface[dsl_x]/ifDescr

This attribute displays the interface description.

telindus24xx/dslInterfaces/interface[dsl_x]/ifType

This attribute displays the interface type. Possible values are:

Value	Description
shdsl	This is displayed in case of a Telindus 2400 SHDSL model.
adsl	This is displayed in case of a Telindus 2400 ADSL model.

telindus24xx/dslInterfaces/interface[dsl_x]/ifOperStatus

This attribute displays the current operational status of the xDSL interface. Possible values are:

Value	Description
up	The xDSL interface is up, data transfer is possible. In case the encapsulation is … • ATM, then the ifOperStatus attribute is up[1] when … - the ATM synchronisation status is synched. - the line is in data state. - the bit pump is synchronised. • PPP, then the ifOperStatus attribute is up[1] when … - LCP is open. - the line is in data state. - the bit pump is synchronised. -
down	The xDSL interface is down, data transfer is not possible.

1. In this case the interface[dsl_x]/alarmInfo/linkDown alarm is off.

Important remarks

- Whether the Telindus 2400 is configured in bridging or routing has no effect on the value of the status attribute ifOperStatus and the alarm attribute linkDown.
- In case of ATM, if OAM F5 loop-back is disabled, then the ifOperStatus of the PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the PVC is configured (correctly) on the remote side. However, the other conditions as stated in the table above remain.
- In case of PPP, if link monitoring is disabled, then it is possible that the ifOperStatus value does not go down even if the link quality is too bad for a proper data link. This because the link monitoring mechanism is the only PPP mechanism that will start a renegotiation of the LCP layer.

14.9.2 SHDSL line status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/line/ifDescr on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/ifType on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/ifOperStatus on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/ifSpeed on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/region on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/numDiscoveredRepeaters on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/eocAlarmThresholds on page 520
- telindus24xx/dslInterfaces/interface[dsl_x]/line/eocStatus on page 520

telindus24xx/dslInterfaces/interface[dsl_x]/line/ifDescr

This attribute displays the interface description.

telindus24xx/dslInterfaces/interface[dsl_x]/line/ifType

This attribute displays the interface type.

telindus24xx/dslInterfaces/interface[dsl_x]/line/ifOperStatus

This attribute displays the current operational status of the line. Possible values are:

Value	Description
up	The line is up, data transfer is possible.
down	The line is down, data transfer is not possible.
testing	A line test is active.

telindus24xx/dslInterfaces/interface[dsl_x]/line/ifSpeed

This attribute displays the current line speed in bits per second (bps).

In case you created a dual pair line, the line/ifSpeed attribute displays the sum of the speed of line pair 1 and 2.

telindus24xx/dslInterfaces/interface[dsl_x]/line/region

This attribute displays the SHDSL standard currently used. Possible values are: auto, annexA, annexB. Refer to telindus24xx/profiles/xdsl/shdsl_default/region on page 356 for more information on these values.

telindus24xx/dslInterfaces/interface[dsl_x]/line/numDiscoveredRepeaters

This attribute displays the number of SHDSL repeaters that the Telindus 2400 discovered on the SHDSL line.

telindus24xx/dslInterfaces/interface[dsl_x]/line/eocAlarmThresholds

This attribute displays the values of the attributes lineAttenuation and noiseMargin as they are configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds attribute on the Telindus 2400 itself.

Also refer to The eocHandling attribute (fixed to alarmConfiguration) on page 102.

telindus24xx/dslInterfaces/interface[dsl_x]/line/eocStatus

This attribute displays the status of the EOC channel.

14.9.3 SHDSL line pair status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/ifOperStatus on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/ifSpeed on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/status on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/timeSinceLastRetrain on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/lineAttenuation on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/noiseMargin on page 524
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/actualBitRate on page 525
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/physLinePair on page 525

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/ifOperStatus

This attribute displays the current operational status of the line pair. Possible values are:

Value	Description
up	The line pair is up, data transfer is possible. This is the case when the value of the linePair/status attribute is dataState.
down	The line pair is down, data transfer is not possible.
testing	A line test is active.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/ifSpeed

This attribute displays the line pair speed, in bits per second (bps), when the line pair is in data state.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/status

This attribute displays the current status of the line pair. Possible values are:

Value	Description
idle	No link is present.
training	A training cycle is in progress.
dataState	A data link is present.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/timeSinceLastRetrain

This attribute displays the elapsed time since the last retrain cycle.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/lineAttenuation

This attribute displays the current line pair attenuation in dB.

The lineAttenuation attribute does not display meaningful information when the line is not trained. It is only relevant for a line that is in data state for at least 5 minutes.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/noiseMargin

This attribute displays the current noise margin on the line pair in dB.

The noiseMargin attribute does not display meaningful information when the line is not trained. It is only relevant for a line that is in data state for at least 5 minutes.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/actualBitRate

This attribute displays the maximum speed, in bits per second (bps), that could be negotiated on the line pair during the training sequence.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/physLinePair

The physLinePair attribute displays the physical index of the line pair.

14.9.4 SHDSL repeater and end status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorId on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorModel on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorSerial on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorSoftVersion on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/eocSoftVersion on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/shdslVersion on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/eocStatus on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/eocAlarmThresholds on page 527
- telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/lineAttenuation on page 528
- telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/noiseMargin on page 528

This section describes the following actions:

- telindus24xx/dslInterfaces/interface[dsl_x]/repeater/loopbackActivation on page 528

telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorId

This attribute displays information about the vendor of the repeater or end device. The vendorId structure contains the following elements:

- countryCode E.g. 65295 for Belgium.
- providerCode E.g. TLS_ for Telindus.
- vendorSpecific

telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorModel

This attribute displays the model of the repeater or end device. E.g. SHDSL TT 2P for a Crocus SHDSL Table Top 2 pair version.

telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorSerial

This attribute displays the serial number of the repeater or end device. For a Telindus devices this is the deviceId attribute (refer to telindus24xx/deviceId on page 484).

telindus24xx/dslInterfaces/interface[dsl_x]/end/vendorSoftVersion

This attribute displays the version of the firmware used on the repeater or end device. For a Telindus device this is the part after "/" of the T-code string displayed in the flashVersion attribute (refer to telindus24xx/flash1Version on page 482).

telindus24xx/dslInterfaces/interface[dsl_x]/end/eocSoftVersion

This attribute displays the EOC software version used on the repeater or end device.

telindus24xx/dslInterfaces/interface[dsl_x]/end/shdslVersion

This attribute displays the SHDSL version used on the repeater or end device.

telindus24xx/dslInterfaces/interface[dsl_x]/end/eocStatus

This attribute displays the state of the EOC channel.

telindus24xx/dslInterfaces/interface[dsl_x]/end/eocAlarmThresholds

This attribute displays the values of the attributes lineAttenuation and noiseMargin as they are configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds attribute on the Telindus 2400 itself.

Also refer to The eocHandling attribute (fixed to alarmConfiguration) on page 102.

telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/lineAttenuation

This attribute displays the line attenuation, in dB, as it is measured on the line pair of the repeater or end device.

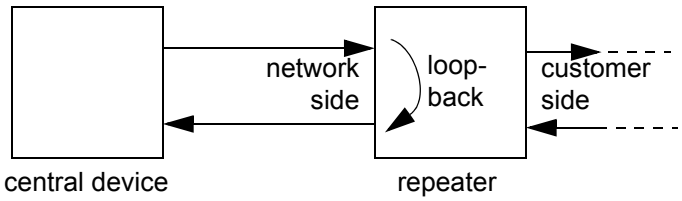
telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/noiseMargin

This attribute displays the noise margin, in dB, as it is measured on the line pair of the repeater or end device.

telindus24xx/dslInterfaces/interface[dsl_x]/repeater/loopbackActivation

This action is only present in the repeater object.

Use this action to set up a loop at the network side of the Crocus SHDSL Repeater:



Set the loop by selecting the action argument value initiateNetworkLoopback and executing the action (in TMA, double-click the loopbackActivation string). Stop the loop by selecting the action argument value clearAllMaintenanceStates and executing the action (in TMA, double-click the loopbackActivation string).

Important remarks

- You can only set up a loop at the network side of the Crocus SHDSL Repeater. Not at the customer side.
- You can only start the loopbackActivation action on the central device (i.e. the Telindus 2400). Not on the remote device.

14.9.5 ADSL line status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_y]/line/ifDescr on page 530
- telindus24xx/dslInterfaces/interface[dsl_y]/line/ifType on page 530
- telindus24xx/dslInterfaces/interface[dsl_y]/line/ifOperStatus on page 530
- telindus24xx/dslInterfaces/interface[dsl_y]/line/ifUsSpeed on page 530
- telindus24xx/dslInterfaces/interface[dsl_y]/line/ifDsSpeed on page 530
- telindus24xx/dslInterfaces/interface[dsl_y]/line/standard on page 530

telindus24xx/dslInterfaces/interface[dsl_y]/line/ifDescr

This attribute displays the interface description.

telindus24xx/dslInterfaces/interface[dsl_y]/line/ifType

This attribute displays the interface type.

telindus24xx/dslInterfaces/interface[dsl_y]/line/ifOperStatus

This attribute displays the current operational status of the line. Possible values are:

Value	Description
up	The line is up, data transfer is possible.
down	The line is down, data transfer is not possible.

telindus24xx/dslInterfaces/interface[dsl_y]/line/ifUsSpeed

This attribute displays the current upstream line speed in bits per second (bps).

telindus24xx/dslInterfaces/interface[dsl_y]/line/ifDsSpeed

This attribute displays the current downstream line speed in bits per second (bps).

telindus24xx/dslInterfaces/interface[dsl_y]/line/standard

This attribute displays which ADSL standard is currently in use. Possible values are: dmt, lite, t1.413.

Concerning the T1.413 standard, refer to the remark in the explanation of the configuration attribute standard (refer to telindus24xx/profiles/xdsl/adsl_default/standard on page 363).

14.9.6 ADSL line pair status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/status on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/progress on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/timeSinceLastRetrain on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/lineAttenuation on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/noiseMargin on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/transmitPower on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/usInterleaveDelay on page 532
- telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/dsInterleaveDelay on page 532

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/status

This attribute displays the current status of the line pair. Possible values are:

Value	Description
idle	No link is present.
training	A training sequence is in progress.
handshake	A handshake sequence is in progress.
dataState	A data link is present.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/progress

This attribute displays the bit-pump its training state machine stages. It shows the progress of the complete training sequence in numerical values (e.g. idle = 0, handshake = 16, training = 32, data state = 208).

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/timeSinceLastRetrain

This attribute displays the elapsed time since the last retrain cycle.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/lineAttenuation

This attribute displays the current line pair attenuation in dB.

The lineAttenuation attribute does not display meaningful information when the line is not trained. It is only relevant for a line that is in data state for at least 5 minutes.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/noiseMargin

This attribute displays the current noise margin on the line pair in dB.

The noiseMargin attribute does not display meaningful information when the line is not trained. It is only relevant for a line that is in data state for at least 5 minutes.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/transmitPower

This attribute displays the current transmit power on the line pair in dB.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/usInterleaveDelay

This attribute displays the current upstream interleave delay in milliseconds.

telindus24xx/dslInterfaces/interface[dsl_y]/line/linePair/dsInterleaveDelay

This attribute displays the current downstream interleave delay in milliseconds.

14.9.7 ADSL end status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorId on page 534
- telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorRevision on page 534
- telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorSerial on page 534
- telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/lineAttenuation on page 534
- telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/noiseMargin on page 534
- telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/transmitPower on page 534

telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorId

This attribute displays information about the vendor of the end device.

telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorRevision

This attribute displays the ADSL revision used on the end device.

telindus24xx/dslInterfaces/interface[dsl_y]/end/vendorSerial

This attribute displays the serial number of the end device.

telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/lineAttenuation

This attribute displays the line attenuation, in dB, as it is measured on the line pair of the end device.

telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/noiseMargin

This attribute displays the noise margin, in dB, as it is measured on the line pair of the end device.

telindus24xx/dslInterfaces/interface[dsl_y]/end/linePair/transmitPower

This attribute displays the current transmit power on the line pair in dB.

14.10 ATM status attributes

This section describes the following status attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/atm/atmSync
- telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc
- telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp

telindus24xx/dslInterfaces/interface[dsl_x]/atm/atmSync

This attribute displays the ATM synchronisation status. Possible values are: synced, notSynced.

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc

This attribute gives the complete status information of all the PVCs (Virtual Channels) that are present on the xDSL interface.

The pvc table contains the following elements:

Element	Description
name	This is the name of the PVC as you configured it. If you did not configure a name, then this element displays: <interface name> “vpi” <vpi number> “vci” <vci number>. E.g. wan vpi 102 vci 102
ifOperStatus	This is the current operational status of the PVC. In case OAM F5 loop-back is … • disabled, i.e. no OAM F5 loop-back cells are sent, then the ifOperStatus of the PVC becomes up when the ATM is synchronised globally. However, this does not guarantee that the PVC is configured (correctly) on the remote side. • enabled, i.e. OAM F5 loop-back cells are sent at regular intervals, then the ifOperStatus of the PVC becomes down when consecutive cells are not returned by the remote side.
ifLastChange	This is the system-up time on the moment the PVC entered its current operational state. I.e. the moment the value of the ifOperStatus element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange element.
ip	This displays the IP information of the PVC. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/ip on page 537 for a detailed description of the ip structure.
bridging	This displays the bridging information of the PVC. Refer to telindus24xx/lanInterface/bridging on page 490 for a detailed description of the bridging structure.
atm	This displays the specific ATM related status information of the PVC. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm on page 538 for a detailed description of the atm structure

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/ip

The ip structure in the pvc table displays the IP information of the PVC.

The ip structure contains the following elements:

Element	Description
address	This is the IP address of the PVC. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the PVC. It is either configured or retrieved automatically.
remote	This is the IP address of the remote end of the PVC. It is either configured or retrieved automatically.

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm

The atm structure in the pvc table displays the specific ATM related status information of the PVC.

The atm structure contains the following elements:

Element	Description
vpi	This displays the Virtual Path Identifier (VPI).
vci	This displays the Virtual Channel Identifier (VCI). The VPI in conjunction with the VCI identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
ppp	This displays the PPP information of the PVC in case you run PPP over ATM. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm/ppp on page 539 for a detailed description of the elements in the ppp structure.

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm/ppp

The ppp structure in the atm structure displays the PPP information of the PVC in case you run PPP over ATM.

The ppp structure contains the following elements:

Element	Description
lcpState	This attribute reflects the status of the LCP (Link Control Protocol) protocol. Possible values are: **Element** / **Description** Initial — LCP handshake has not started yet. Starting, Closed, Stopped, Closing, Stopping — These values correspond with the transient states in the LCP state diagram. Req-Sent — The local side of the PPP link has sent an LCP request. The remote side did not answer yet. Ack-Rcvd — The local side of the PPP link has received an LCP acknowledge from the remote side. This is a transient state. Ack-Sent — The local side of the PPP link has acknowledged the LCP request from the remote side. Opened — The LCP handshake succeeded.
ipcpState	This attribute reflects the status of the IPCP (Internet Protocol Control Protocol) protocol. The possible values are the same as those of lcpState element.
bcpState	This attribute reflects the status of the BCP (Bridging Control Protocol) protocol. The possible values are the same as those of lcpState element.
ccpState	This attribute reflects the status of the CCP (Compression Control Protocol) protocol. The possible values are the same as those of lcpState element.
myCompressionRatio	When PPP compression is enabled, this attribute displays the compression ratio achieved by the router at this side (local side) of the link.
hisCompressionRatio	When PPP compression is enabled, this attribute displays the compression ratio achieved by the router at the other side (remote side) of the link.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>myAuthenState</td><td>This attribute displays the authentication state of the router at this side (local side) of the link. I.e. the state of the authenticator. Possible values are:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>No-Authentication</td><td>The local side does not request PPP authentication or still has to start the CHAP authentication (LCP handshake is busy).</td></tr>
<tr><td>Wait-On-Response</td><td>The local side has sent a challenge packet and is waiting for an answer.</td></tr>
<tr><td>Authen-Successful</td><td>The response packet is found to be correct. This is the state when authentication succeeded.</td></tr>
<tr><td>Authen-Failure</td><td>The response packet is found to be incorrect. This is a transient state since the router starts the LCP handshake again after a failing authentication.</td></tr>
</table></td></tr>
<tr><td>hisAuthenState</td><td>This attribute displays the authentication state of the router at the other side (remote side) of the link. I.e. the state of the peer. Possible values are:
<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>No-Authentication</td><td>This is the start-up state.</td></tr>
<tr><td>Wait-On-Challenge</td><td>During the LCP handshake the authenticator already indicates it wants to authenticate. From that moment on, the peer awaits a challenge packet.</td></tr>
<tr><td>Wait-On-Success</td><td>Once the peer has sent a response, it awaits a success or failure message.</td></tr>
<tr><td>Authen-Successful</td><td>The peer has received a success packet. It remains in this state during data transfer.</td></tr>
<tr><td>Authen-Failure</td><td>The peer has received a failure packet. This is a transient state since the router starts the LCP handshake again after a failing authentication.</td></tr>
<tr><td>Authen-Not-Allowed</td><td>This state only occurs when the peer does not accept the authentication request during the LCP handshake. A possible reason might be that the peer router does not support CHAP.</td></tr>
</table></td></tr>
</table>

telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp

This attribute gives the complete status information of all the VPs (Virtual Paths) that are present on the xDSL interface.

The vp table contains the following elements:

Element	Description
vpi	This is the Virtual Path Identifier (VPI).
ifOperStatus	This is the current operational status of the Virtual Path. In case OAM F4 loop-back is … • disabled, i.e. no OAM F4 loop-back cells are sent, then the ifOperStatus of the VP becomes up when the ATM is synchronised globally. However, this does not guarantee that the VP is configured (correctly) on the remote side. • enabled, i.e. OAM F4 loop-back cells are sent at regular intervals, then the ifOperStatus of the VP becomes down when consecutive cells are not returned by the remote side.

14.11 Profile status attributes

All the different profile objects (SHDSL, ADSL, ATM PVC, application and configuration profiles) only contain one and the same status attribute.

This section describes the following status attributes:

- telindus24xx/profiles/<profileName>/profileUsers on page 543

telindus24xx/profiles/<profileName>/profileUsers

This attribute shows where the current profile is applied. The profileUsers table can contain the following elements:

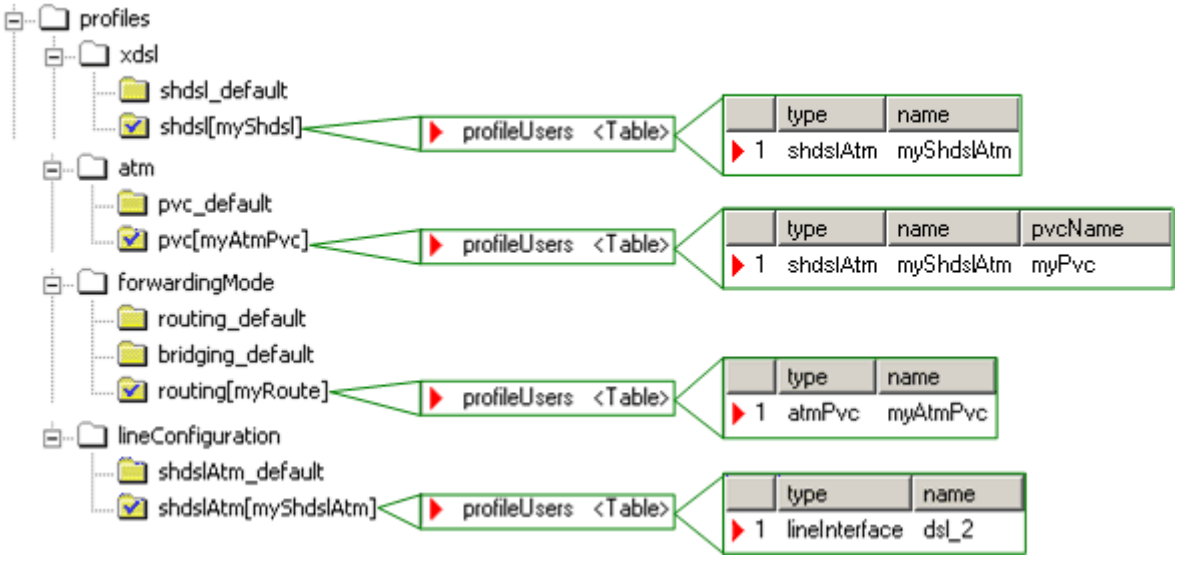
Element	Description
type	This is the type of profile on which the current profile is applied. For example: • If for the forwardingMode/routing_default profile the type element displays atmPvc, it means that the routing_default profile has been applied on an ATM PVC profile. • If for the lineConfiguration/xdslAtm_default profile the type element displays lineInterface, it means that the xdslAtm_default profile has been applied on an xDSL line interface.
name	This is the name of the profile on which the current profile is applied. It is the index name you assigned to the profile when you created it.
pvcName	This element is only present in case of an ATM PVC profile. This is the name of the PVC on which the ATM PVC profile is applied.

Example

Suppose …

- the forwardingMode/routing[myRoute] profile is applied on the atm/pvc[myAtmPvc] profile.
- the atm/pvc[myAtmPvc] profile and xdsl/shdsl[myShdsl] profile are applied on the lineConfiguration/shdslAtm[myShdslAtm] profile. What is more, the atm/pvc[myAtmPvc] profile is applied on a PVC with name myPvc.
- the lineConfiguration/shdslAtm[myShdslAtm] profile is applied on the interface[dsl_2] SHDSL line interface.

In that case, the profileUsers table of the different profiles indicate the following:



14.12 Router status attributes

This section discusses the status attributes concerned with routing. First it describes the general routing status attributes such as routingTable, etc. Then it explains the status attributes of the extra features such as address translation, L2TP tunnelling, etc.

The following gives an overview of this section:

- 14.12.1 - General router status attributes on page 545
- 14.12.2 - Default NAT status attributes on page 553
- 14.12.3 - L2TP tunnel status attributes on page 555

14.12.1 General router status attributes

This section describes the following status attributes:

- telindus24xx/ip/router/routingTable on page 546
- telindus24xx/ip/router/igmpTable on page 548
- telindus24xx/ip/router/dhcpBinding on page 550
- telindus24xx/ip/router/dhcpStatistics on page 550
- telindus24xx/ip/router/dhcpRelayInfo on page 551
- telindus24xx/ip/router/radius on page 551
- telindus24xx/ip/router/dns on page 551
- telindus24xx/ip/router/addrPools on page 552

telindus24xx/ip/router/routingTable

This attribute lists *all* known routes (both static and learned) with their operating status.

The routingTable contains the following elements:

Element	Description
network	This is the IP address of the destination network.
mask	This is the network mask of the destination network.
gateway	This is the IP address of the next router on the path to the destination network.
interface	This is the interface through which the destination network can be reached. Possible values are: **Value** / **Description** internal: The own protocol stack is used. <name>: The destination network can be reached through this particular interface. The <name> of the interface is the name as you configured it. Note that the "interface" can also be a DLCI, an ATM PVC, a tunnel, etc. discard: Packets for this destination are discarded.
encapsulation	This is the used encapsulation. It is related to the interface for this route. Possible values are: **Value** / **Description** none: The IP packets are not encapsulated. ethernet: The IP packets are encapsulated with the ARPA MAC header. atm: The IP packets are encapsulated in ATM. ppp: The IP packets are encapsulated in PPP. frameRelay: The IP packets are encapsulated in Frame Relay (RFC 1490).
status	This is the route status. Possible values are: **Value** / **Description** up: The route can be used. down: The route is currently not in use. discard: Packets for this destination are discarded.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>preference</td><td>This displays the route preference. If more than one route matches the IP destination address, this attribute determines which route is used. The route with the lowest preference value will be used.</td></tr>
<tr><td>type</td><td>This is the type of the route. Possible values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>host</td><td>This is a host route, i.e. a route to a single IP address instead of a complete network. This is also used for the router its own IP address.</td></tr>
<tr><td>internal</td><td>A route with this status is irrelevant.</td></tr>
<tr><td>local</td><td>This route is for directly connected networks.</td></tr>
<tr><td>rip</td><td>This route has been received by a RIP update.</td></tr>
<tr><td>static</td><td>This route has been configured, i.e. it is a static route.</td></tr>
</table>
</td></tr>
<tr><td>metric</td><td>If two routes exist with the same preference, then the route with the lowest metric value is chosen. The metric attribute serves as a cost for using the route. In most cases it indicates the number of hops (= routers) required to reach a destination.</td></tr>
<tr><td>timeOut</td><td>In case of a RIP route, the timeOut attribute displays the time the route will remain in the routing table if no RIP updates are received anymore. For other routes this attribute always displays 00000d 00h 00m 00s.</td></tr>
</table>

telindus24xx/ip/router/igmpTable

This attribute shows the multicast address, reported by one or more clients. The igmpTable is always updated, even if no proxy is configured.

The igmpTable contains the following elements:

Element	Description
multicast	This is the multicast address.
interface	This is the interface name of the client(s). In case of multiple interface names, they are separated from each other by a comma.

What is IGMP?

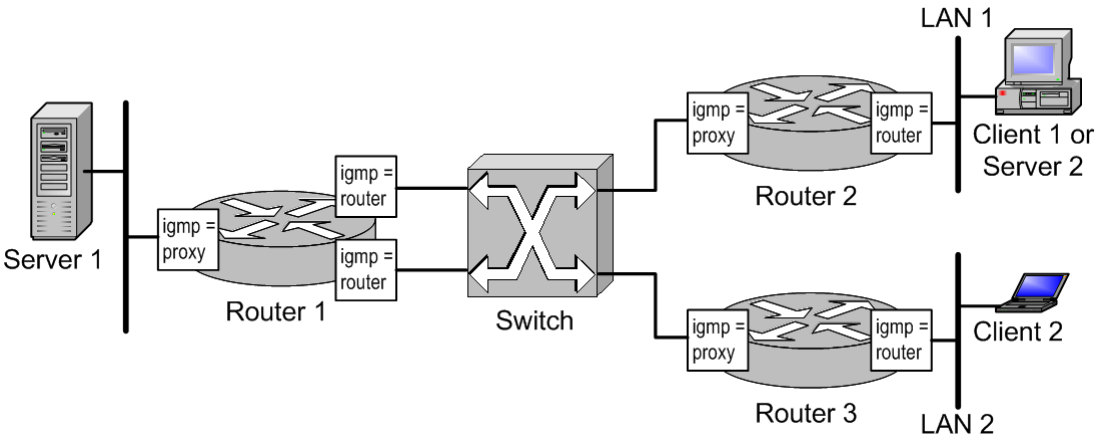
Internet Group Management Protocol (IGMP) is defined in RFC 1112 as the standard for IP multicasting in the Internet.

It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group.

All hosts conforming to level 2 of the IP multicasting specification require IGMP.

IGMP topology

Consider the following multicasting topology:



In this topology …

- Client 1 and Client 2 are multicast clients.
- Router 1, 2 and 3 are multicast enabled routers.
- Server 1 is a multicast server.
- Switch is a Frame Relay or ATM switch.

The following are some characteristics of an IGMP topology:

- An IGMP router queries an IGMP proxy.
- Only 1 IGMP proxy can be defined per device.
- The TTL of an IGMP frame is always 1. IGMP messages are never forwarded.
- An IGMP frame contains an IP router alert option.
- IGMPv1 routers may be present in the network.

The multicasting IGMP protocol can be configured on every IP interface. Refer to the igmp element in 6.2.3 - Explaining the ip structure on page 90.

A client can leave or join a multicast group by erasing or adding a multicast address from a table, defined in the client application. A list of multicast group addresses is maintained in the routers. The reported multicast addresses can be seen in the igmpTable. Refer to telindus24xx/ip/router/igmpTable on page 548.

Multicast frames are always forwarded on the proxy interface. Therefore, in the IGMP topology example, it is also possible to add a multicast server (Server 2) on LAN 1. Client 2 can join a multicast group of Server S2.

Since IGMP is send in UDP (join/leave can be lost), the clients (proxies) are polled every 125 seconds:

- A general query is send to 224.0.0.1 (poll all systems).
- A leave group message is send to 224.0.0.2 (all routers).

telindus24xx/ip/router/dhcpBinding

This attribute contains a list of dynamically assigned (i.e. leased) IP addresses.

The dhcpBinding table contains the following elements:

Element	Description
ipAddress	This is the IP address that is dynamically assigned to a client.
macAddress	This is the MAC address of the client.
leaseTime	This is the remaining lease time.

telindus24xx/ip/router/dhcpStatistics

This attribute contains the statistics of all IP address ranges that have been specified in the configuration attribute telindus24xx/ip/router/dhcpDynamic.

The dhcpStatistics table contains the following elements:

Element	Description
startRange	Displays the IP start address of an IP address range.
endRange	Displays the IP end address of an IP address range.
free	For the corresponding IP address range, this displays the number of IP addresses that are still free.
lease	For the corresponding IP address range, this displays the number of IP addresses that are leased.
hold	For the corresponding IP address range, this displays the number of IP addresses that are on hold.

During power-down of the Telindus 2400, some leased IP addresses can still be active. Because the duration of the power-down can not be known, all timer information about lease and hold time becomes meaningless. Therefore, the DHCP server incorporated in the Telindus 2400 sends a ping to all leased addresses after a warm boot. When the client responds to this ping, the DHCP server resets all timers to their default value and keeps the lease with this client.

telindus24xx/ip/router/dhcpRelayInfo

This attribute displays the status information of the DHCP relay process in case the Telindus 2400 is configured to act as DHCP relay agent (refer to 12.1.4 - Configuring the Telindus 2400 as DHCP relay agent on page 270).

The dhcpRelayInfo table contains the following elements:

Element	Description
sourceIntf	This is the name of the interface on which the DHCP request has been received.
mac	This is the MAC address of the client.
assignedIp	This is the IP address that has been dynamically assigned to the client by the remote DHCP server.
serverIp	This is the IP address of the remote DHCP server.
dhcpStatus	This is the status of the DHCP process. Possible values are: discover, offer, request, decline, ack, nack, release, inform, idle.
leaseTime	This is the remaining lease time.

telindus24xx/ip/router/radius

This attribute shows some RADIUS status information. Refer to What is RADIUS? on page 418 for more information.

The radius structure contains the following elements:

Element	Description
authServer	This is the IP address of the authentication server the Telindus 2400 is connected to.
acctServer	This is the IP address of the accounting server the Telindus 2400 is connected to.
pendingRequests	This is the amount of pending requests on these servers.

telindus24xx/ip/router/dns

This attribute shows some DNS status information. Refer to What is DNS? on page 418 for more information.

The dns table contains the following elements:

Element	Description
ipAddress	This is the IP address of the DNS server.
hostname	This is the hostname of the DNS server.
ttl	This is the time-to-live of the cached DNS data.

telindus24xx/ip/router/addrPools

This attribute shows which IP addresses have already been picked out of the IP address pool. Refer to What is an IP address pool? on page 91 for more information.

The addrPools table contains the following elements:

Element	Description
name	This is the name of the IP address pool, as you configured it, from which the IP addresses have been picked.
type	This is the type of IP address pool from which the IP addresses have been picked. Possible values are: list or interval.
local	This is the local IP address that has been picked out of the IP address pool.
remote	This is the remote IP address that has been picked out of the IP address pool.
netMask	This is the subnet mask that has been picked out of the IP address pool.
interface	This is the name of the interface on which the IP addresses are used.

14.12.2 Default NAT status attributes

This section describes the following status attributes:

• telindus24xx/ip/router/defaultNat/addresses on page 554

telindus24xx/ip/router/defaultNat/addresses

This attribute displays the status of each official IP address that is configured in the configuration attribute telindus24xx/ip/router/defaultNat/addresses.

The addresses table contains the following elements:

Element	Description
officialAddress	This is the official IP address as you entered it in the addresses configuration attribute.
privateAddress	This is the private IP address that is currently linked with the official IP address.
status	This is the status of the official IP address. Possible values are: **Value** / **Description** free — This official IP address is currently not in use. fixed — This address has a pre-configured mapping between the official and private IP address. allocated — This official IP address is currently assigned to a private IP address, but it is not fixed.
uses	This indicates how many sessions are currently used by this official IP address. If the attribute value becomes zero, the assigned official IP address becomes free again and can be assigned to another private IP address.

14.12.3 L2TP tunnel status attributes

This section describes the following status attributes:

- telindus24xx/ip/router/tunnels/l2tpTunnels on page 556
- telindus24xx/ip/router/tunnels/ipsecL2tpTunnels on page 557

telindus24xx/ip/router/tunnels/l2tpTunnels

This attribute displays status information of the L2TP tunnels.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel as you configured it. If you did not configure a name, then this element displays: “tunnel” <local IP address of the tunnel>. E.g. tunnel 192.168.5.1
ifOperStatus	This displays the operational status of the tunnel. Possible values are: **Value** / **Description** up — The tunnel is up, data transfer is possible. down — The tunnel is down, data transfer is not possible. dormant — The tunnel is "stand-by". As soon as data has to be sent over the tunnel, control connect messages are exchanged and the operational status of the tunnel becomes up.
ifLastChange	This is the system-up time on the moment the tunnel entered its current operational state. I.e. the moment the value of the ifOperStatus status element changes (from up to down or vice versa), the system-up time value is written into the ifLastChange status element.
ip	This displays the IP information of the tunnel. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/ip on page 537 for a detailed description of the ip structure.
bridging	This displays the bridging information of the tunnel. Refer to telindus24xx/lanInterface/bridging on page 490 for a detailed description of the bridging structure.
l2tp	This displays the specific L2TP related status information of the tunnel. Refer to the telindus24xx/ip/router/tunnels/l2tpTunnels/l2tp on page 557 for a detailed description of the l2tp structure.
ppp	This displays the PPP information of the tunnel. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm/ppp on page 539 for a detailed description of the elements in the ppp structure.

telindus24xx/ip/router/tunnels/l2tpTunnels/l2tp

The l2tp structure in the l2tpTunnels table displays the specific L2TP related status information of the tunnel.

The l2tp structure contains the following elements:

Element	Description
txSeqNum	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the transmit data sequence numbers.
rxSeqNum	In case sequence numbering on the data messages is enabled (dataChannelSequenceNumbering = on), then this displays the receive data sequence numbers.
mode	This displays which L2TP server type the Telindus 2400 currently is: LAC or LNS. If you set the configuration attribute mode to auto, then the mode status attribute displays the auto value until the Telindus routers have mutually decided who will be the LAC and who the LNS.
controlState	This displays the states associated with the LNS or LAC control connection establishment. Refer to L2TP status - control states on page 558 for more information.
callState	This displays the states associated with the LNS or LAC incoming or outgoing calls. Refer to L2TP status - call states on page 559 for more information.
deliveryState	This displays the states associated with the LNS or LAC packet delivery. Refer to L2TP status - delivery states on page 560 for more information.
authenState	This displays the states associated with the LNS or LAC authentication. Refer to L2TP status - authentication states on page 561 for more information.

telindus24xx/ip/router/tunnels/ipsecL2tpTunnels

This attribute displays status information of the IPSEC L2TP tunnels.

The ipsecL2tpTunnels table contains the same elements as the l2tpTunnels table. Refer to telindus24xx/ip/router/tunnels/l2tpTunnels on page 556.

L2TP status - control states

The states associated with the LNS or LAC for control connection establishment are:

Value	Description
idle	No control connection is present. Both initiator and recipient start from this state. An initiator transmits a Start Control Connection Request, while a recipient remains in the idle state until receiving a Start Control Connection Request.
waitCtlReply	This is the state where a Start Control Connection Reply is awaited.
waitCtlConn	This is the state where a Start Control Connection Connected is awaited. Upon receipt, the challenge response is checked. The tunnel either is established, or is torn down if an authorisation failure is detected.
established	The control connection is established. An established connection may be terminated by either a local condition or the receipt of a Stop Control Connection Notification. The session then returns to the idle state.

L2TP status - call states

The states associated with the LNS or LAC incoming or outgoing calls are:

Value	Description
idle	No data is exchanged over the tunnel.
waitTunnel	This is the state in which is waited … • either for the control connection to be opened, • or for verification that the tunnel is already open. Once an indication is received that the tunnel has/was opened, session control messages may be exchanged. The first of these is the Incoming Call Request.
waitReply	This is the state where an Incoming or Outgoing Call Reply message is awaited. If an Incoming or Outgoing Call Reply message is received, an incoming or Outgoing Call Connected message is sent and the session moves to the established state.
waitConnect	This is the state where an Incoming or Outgoing Call Connected message is awaited. If an Incoming or Outgoing Call Connected message is received, the call was successful and the session moves to the established state.
established	Data is exchanged over the tunnel. The session is terminated when receiving or sending a Call Disconnect Notify message. The session then returns to the idle state.

L2TP status - delivery states

The states associated with the packet delivery are:

Value	Description
operating	The Telindus 2400 has sent a packet, but has not received an acknowledgement on this packet yet.
idle	All transmitted packets have been acknowledged.

L2TP status - authentication states

The states associated with the LNS or LAC authentication are:

Value	Description
noAuthentication	Authentication is not enabled. This is also the start-up state for the authentication process.
authenSuccessful	Authentication was successful. The Telindus 2400 remains in this state during data transfer.
authenFailure	Authentication failed. This is a transient state since the Telindus 2400 starts the handshake again after a failing authentication.

14.13 Bridge group status attributes

This section describes the following status attributes:

- telindus24xx/bridge/bridgeGroup/ifDescr on page 563
- telindus24xx/bridge/bridgeGroup/ifType on page 563
- telindus24xx/bridge/bridgeGroup/ifOperStatus on page 563
- telindus24xx/bridge/bridgeGroup/ifMtu on page 563
- telindus24xx/bridge/bridgeGroup/ip on page 563
- telindus24xx/bridge/bridgeGroup/macAddress on page 563
- telindus24xx/bridge/bridgeGroup/arpCache on page 564
- telindus24xx/bridge/bridgeGroup/bridgeCache on page 565
- telindus24xx/bridge/bridgeGroup/bridging on page 566
- telindus24xx/bridge/bridgeGroup/spanningTree on page 566

This section describes the following actions:

- telindus24xx/bridge/bridgeGroup/clearArpCache on page 568
- telindus24xx/bridge/bridgeGroup/clearBridgeCache on page 568

telindus24xx/bridge/bridgeGroup/ifDescr

This attribute displays the interface description.

telindus24xx/bridge/bridgeGroup/ifType

This attribute displays the interface type.

telindus24xx/bridge/bridgeGroup/ifOperStatus

This attribute displays the current operational status of the bridge group.

telindus24xx/bridge/bridgeGroup/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

telindus24xx/bridge/bridgeGroup/ip

This attribute displays the IP information of the bridge.

The ip structure contains the following elements:

Element	Description
address	This is the IP address of the bridge. It is either configured or retrieved automatically.
netMask	This is the IP subnet mask of the interface. It is either configured or retrieved automatically.

telindus24xx/bridge/bridgeGroup/macAddress

This attribute displays the MAC address of the bridge group.

telindus24xx/bridge/bridgeGroup/arpCache

This attribute displays all the MAC address - IP address pairs from ARP requests and replies received on the LAN interface. Refer to What is the ARP cache? on page 314 for more information.

The arpCache table contains the following elements:

Element	Description
macAddress	This is the MAC address.
ipAddress	This is the associated IP address.
type	This is the ARP cache entry type. Possible values are: **Value** / **Description** dynamic: The MAC - IP address pair is retrieved from an ARP request or reply message. static: The MAC - IP address pair is configured. There is only one static entry, i.e. the Telindus 2400 its own IP and MAC address.
timeOut	This is the time the entry will remain in the ARP cache. For the static entry, this value is 0.

telindus24xx/bridge/bridgeGroup/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the network that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database. Refer to What is the bridge cache? on page 448 for more information.

The bridgeCache table contains the following elements:

Element	Description
interface	This is the interface through which the station can be reached.
macAddress	This is the MAC address of the station situated on the network connected to the interface.
type	This displays whether the MAC address entry is static or dynamic: **Value** / **Description** dynamic: The corresponding MAC address is learned on one of the interfaces. static: There are only two static entries: • the Telindus 2400 its own MAC address. • a MAC address used for Spanning Tree.
age	This is the elapsed time since a frame was received from the station.

Example

The following figure shows part of a bridge cache table as an example:

bridgeCache

	interface	macAddress	type	age
1	Bridge Protocol Entity	01:80:c2:00:00:00	static	00000d 00h 00m 00s
2	Bridge Protocol Entity	00:c0:89:00:fe:20	static	00000d 00h 00m 00s
3	lan	00:c0:89:00:d4:56	dynamic	00000d 00h 00m 01s
4	lan	00:c0:89:00:70:98	dynamic	00000d 00h 00m 09s
5	lan	00:c0:89:00:6b:9c	dynamic	00000d 00h 00m 16s
6	lan	00:c0:89:01:26:86	dynamic	00000d 00h 00m 05s
7	lan	00:10:b5:ec:3f:24	dynamic	00000d 00h 00m 00s
8	lan	00:a0:24:a2:97:6c	dynamic	00000d 00h 01m 25s
9	lan	00:c0:89:00:d4:53	dynamic	00000d 00h 01m 53s
10	lan	00:60:8c:95:bb:fe	dynamic	00000d 00h 00m 00s
11	lan	00:10:4b:47:38:fa	dynamic	00000d 00h 00m 15s
12	lan	00:c0:89:00:d4:c2	dynamic	00000d 00h 01m 40s

telindus24xx/bridge/bridgeGroup/bridging

The bridging attributes or elements in the individual interface objects display the bridging information for that particular interface. This bridging attribute, however, displays the bridging information of all the (bridged) interfaces of the Telindus 2400.

Refer to telindus24xx/lanInterface/bridging on page 490 for a detailed description of the bridging structure. Note however that the bridge group bridging structure contains one extra element: name. This is the name of the interface as you configured it. Note that the interface can also be a DLCI, an ATM PVC, a tunnel, etc.

telindus24xx/bridge/bridgeGroup/spanningTree

This attribute gives you the Spanning Tree status information of the bridge.

The spanningTree structure contains the following elements:

Element	Description
designatedPriority	Together, these two elements form the unique bridge identifier.
designatedMAC	They display the unique bridge identifier of the root bridge as it is indicated in the root identifier parameter of the Configuration BPDUs. These BPDUs are transmitted by the designated bridge for the LAN that is currently connected to this port. This bridge identifier is used to test the value of the root identifier parameter conveyed in received Configuration BPDUs.
rootPathCost	This is the cost of the path from this bridge to the root bridge. If this bridge is the root bridge, the rootPathCost value equals 0. Else, the rootPathCost value equals the sum of … • the path cost as it is up to the designated bridge for the LAN that is currently connected to this port (this cost is transmitted in Configuration BPDUs by the designated bridge) and • the path cost as it is configured for the root port. The rootPathCost element is used … • to test the value of the root path cost parameter conveyed in received Configuration BPDUs. • as the value of the root path cost parameter in transmitted Configuration BPDUs. The total cost of the path to the root bridge should not exceed 65500.
rootPort	This is the port identifier of the port that offers the lowest cost path to the root. If two or more ports offer equal least cost paths to the root bridge, then the root port is selected to be that with the highest designatedPriority (i.e. the lowest numerical value). If two or more ports offer equal least cost paths to the root bridge and the same designatedPriority, then the root port is selected to be that with the highest designatedPortPriority (i.e. the lowest numerical value).

Element	Description
bridgePriority	Together, these two attributes form the unique bridge identifier of this bridge.
bridgeMAC	
maxAge	This is the time-out value to be used by all bridges in the bridged LAN for discarding bridging information. The maxAge element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value against which to test the age of stored configuration information.
helloTime	This is the interval between the generation of Configuration BPDUs by the root bridge. The helloTime element displays the value as it is set by the root bridge. This attribute is not directly used by the Spanning Tree algorithm, but it is conveyed by the root bridge to facilitate the monitoring of protocol performance by the management system.
forwardDelay	This is the time-out value to be used by all bridges in the bridged LAN for … • a bridge port applies to move from listening state to learning state or from learning state to forwarding state. • time-out (or ageing) for purging MAC addresses from the bridge cache in case a topology change is detected. The forwardDelay element displays the value as it is set by the root bridge. This information is conveyed by the root bridge to ensure that each bridge in the bridged LAN has a consistent value for the forward delay timer.
topologyChange	This is a Boolean value (0 or 1) to report … • for a bridge that is not a root bridge, whether or not the most recently accepted Configuration BPDU indicates a change in the active topology. • for the root bridge, whether or not a change in topology has been detected within the preceding topologyChangeTime period. The topologyChange element is used to … • propagate the topology change indication in transmitted Configuration BPDUs. • determine whether the short (bridgeForwardDelay) or long (bridgeTimeOut) time-out (or ageing) value is used to purge dynamic MAC addresses from the bridge cache.
topologyChange-Detection	This is a Boolean value (0 or 1) to report that a topology change has been detected by or notified to the bridge.
topologyChange-Time	This displays the time during which the root bridge transmits Configuration BPDUs indicating a topology change, after it detected this topology change. The topologyChangeTime element value is equal to the sum of the root bridge its bridgeMaxAge element value and bridgeForwardDelay element value. Refer to telindus24xx/bridge/bridgeGroup/spanningTree on page 449 for more information on the latter two elements.

telindus24xx/bridge/bridgeGroup/clearArpCache

If you execute this action, the ARP cache table is cleared.

telindus24xx/bridge/bridgeGroup/clearBridgeCache

If you execute this action, the bridge cache table is cleared.

14.14 Management status attributes

This section describes the following status attributes:

- telindus24xx/management/cms2Address on page 570
- telindus24xx/management/timeServer on page 570
- telindus24xx/management/alarmLog on page 570

telindus24xx/management/cms2Address

This attribute displays the absolute device address as you configured it.

telindus24xx/management/timeServer

This attribute displays the status of the SNTP time server.

The timeServer structure contains the following elements:

Element	Description
state	This is the state of the connection with the time server.
stratum	This is the stratum level of the time server its reference clock. Possible values are: • 0 : unspecified or unavailable • 1 : primary reference (e.g. radio clock) • 2 - 15 : secondary reference (via SNTP)
delay	This is the total roundtrip delay of the time server with its reference clock.

telindus24xx/management/alarmLog

This attribute displays the alarm log or alarm history. It displays the 32 most recent alarms that occurred on the Telindus 2400.

The alarmLog table contains the following elements:

Element	Description
timeStamp	This is the value of the real time clock at the moment the alarm was generated.
sysUpTime	This is the system up-time of the Telindus 2400 at the moment the alarm was generated.
totalAlarmLevel	This is the total alarm level of the Telindus 2400.
alarmLevel	This is the alarm level of the alarm.
alarm	This is the alarm itself in the format path.alarmName on|off (e.g. telindus24xx/lanInterface.linkDown on).

14.15 Loopback status attributes

This section describes the following status attributes:

- telindus24xx/management/loopback/ifDescr on page 572
- telindus24xx/management/loopback/ifType on page 572
- telindus24xx/management/loopback/ifOperStatus on page 572
- telindus24xx/management/loopback/ifMtu on page 572
- telindus24xx/management/loopback/ipAddress on page 572

telindus24xx/management/loopback/ifDescr

This attribute displays the interface description.

telindus24xx/management/loopback/ifType

This attribute displays the interface type.

telindus24xx/management/loopback/ifOperStatus

This attribute displays the current operational status of the loop-back interface.

The loop-back interface is always up.

telindus24xx/management/loopback/ifMtu

This attribute displays the interface its Maximum Transfer Unit, i.e. the maximum number of bytes that one packet can contain on this interface.

telindus24xx/management/loopback/ipAddress

This attribute displays the IP address of the loop-back interface as you configured it.

14.16 File system status attributes

This section describes the following status attributes:

- telindus24xx/fileSystem/fileList on page 574
- telindus24xx/fileSystem/freeSpace on page 574
- telindus24xx/fileSystem/status on page 574
- telindus24xx/fileSystem/corruptBlocks on page 574

This section describes the following actions:

- telindus24xx/fileSystem/Delete File on page 575
- telindus24xx/fileSystem/Rename File on page 575

telindus24xx/fileSystem/fileList

Part of the flash memory of the Telindus 2400 is organised as a file system and a number of files are stored in it. The fileList attribute shows all the files that are present on the file system. Usually, the following files are present:

- The configuration file of the Telindus 2400 (file config1.db).
- Up to two application software files of the Telindus 2400 (files CONTROL1 and CONTROL 2).

The fileList table contains the following elements:

Element	Description
name	This is the file name. Maximum length of the file name is 24 characters. All characters are allowed (including spaces). The file name is case sensitive.
length	This is the length of the file in bytes.

telindus24xx/fileSystem/freeSpace

This attribute displays the number of free bytes on the file system.

telindus24xx/fileSystem/status

This attribute displays the status of the file system. Possible values are:

Value	Description
ready	Normal situation.
formatting	The file system is being formatted. This can be triggered when the file system is found to be corrupt at boot.
corrupt	The file system is in a state were no guarantee can be given about the correct operation of the file system. The file system will be formatted at the following boot.
corruptBlocks	A certain block can not be erased.

telindus24xx/fileSystem/corruptBlocks

The file system of the Telindus 2400 consists of several blocks. When a block can not be erased, the corruptBlocks count is incremented. This block can no longer be used to store data.

telindus24xx/fileSystem/Delete File

Use this action to remove obsolete files from the file system. You have to enter the file name you want to delete as argument value.

File names are case sensitive.

telindus24xx/fileSystem/Rename File

Use this action to rename a file on the file system. You have to enter the old and new file name in a structure.

File names are case sensitive.

14.17 Operating system status attributes

This section describes the following status attributes:

• telindus24xx/operatingSystem/taskInfo on page 577

telindus24xx/operatingSystem/taskInfo

This attribute displays status information about the operating system.

The taskInfo table contains the following elements:

Element	Description
taskName	This is the name of the task.
taskStatus	This is the current status of the task. Possible values are: **Value** / **Description** awake — This task is actually running. asleep — This task is waiting on an event. inactive — This task slot is not active, i.e. no task has been assigned to this slot.
load30s	This is the load on the processor, in percent, during the last 30 seconds.
load5m	This is the load on the processor, in percent, during the last 5 minutes.
runningInMedium	Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with medium priority during the last 30 seconds.
runningInHigh	Each task can be running with a low, medium or high priority. This element gives the percentage of time this task has been running with high priority during the last 30 seconds. The percentage of time this task has been running with low priority can be calculated using the following formula: running in low priority = 100% - runningInMedium - runningInHigh
programCounter	This is the current value of the program counter. The program counter is the memory address for the current instruction of this task.

15 Performance attributes

This chapter discusses the performance attributes of the Telindus 2400. The following gives an overview of this chapter:

- 15.1 - Performance attributes overview on page 580
- 15.2 - LAN interface performance attributes on page 585
- 15.3 - 4 port Ethernet interface performance attributes on page 589
- 15.4 - 6E1 interface performance attributes on page 590
- 15.5 - E3/T3 interface performance attributes on page 595
- 15.6 - IMA group performance attributes on page 601
- 15.7 - xDSL interface performance attributes on page 603
- 15.8 - ATM performance attributes on page 613
- 15.9 - Router performance attributes on page 617
- 15.10 - Bridge performance attributes on page 629
- 15.11 - Management performance attributes on page 634
- 15.12 - Operating system performance attributes on page 637

15.1 Performance attributes overview

> telindus24xx

>> lanInterface

- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- h2Performance
- h24Performance

>> 4pEth

- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- h2Performance
- h24Performance

>> hexE1

>>> e1[E1_x]

- h2G703Performance
- h24G703Performance
- d7G703Performance
- g703Performance
- h2G826Performance
- h24G826Performance
- d7G826Performance
- g826Performance
- tcPerformance

>> e3T3

>>> e3T3[E3T3_x]
h2G703Performance
h24G703Performance
d7G703Performance
g703Performance
h2G826Performance
h24G826Performance
d7G826Performance
g826Performance

>>>> atm
pvc
vp
unknownCells

>> bundle

>>> imaGroup[ ]
pvc
members

>> dslInterfaces

>>> interface[dsl_x]

>>>> line
h2Line
h24Line
d7Line
line
Action: retrain[1]

>>>>> linePair
h2LineParameters
h2Performance
h24LineParameters
h24Performance
d7LineParameters
d7Performance
lineParameters
performance

1. Telindus 2400 SHDSL models only (2421, 2422, 2423).

>>> repeater[2]

>>>> networkLinePair

- h2LineParameters
- h2Performance
- h24LineParameters
- h24Performance
- d7LineParameters
- d7Performance
- lineParameters
- performance

>>>> customerLinePair

- h2LineParameters
- h2Performance
- h24LineParameters
- h24Performance
- d7LineParameters
- d7Performance
- lineParameters
- performance

>>> end

>>>> linePair

- h2LineParameters
- h2Performance
- h24LineParameters
- h24Performance
- d7LineParameters
- d7Performance
- lineParameters
- performance

>>> atm

- pvc
- vp
- uniStatistics

2. Telindus 2400 SHDSL models only (2421, 2422, 2423).

>> ip

>>> router
routingTable
radiusAuth
radiusAcct
pingResults
Action: startPing
Action: stopPing

>>>> defaultNat
socketsFree
allocFails
discards
addressesAvailable
tcpSocketsUsed
udpSocketsUsed
icmpSocketsUsed
tcpAllocs
udpAllocs
icmpAllocs
Action: resetNat

>>>> tunnels
l2tpTunnels
ipsecL2tpTunnels

>>>> manualSA[ ]
inPackets
outPackets
espAuthenticationFailure
espDecryptionFailure
espSequenceNrReplay
espDroppedFrames

>>>> routingFilter[ ]
filter

>> bridge

>>> bridgeGroup
bridgeCache
bridgeDiscards
bridgeFloods

>>> accessList[ ]
bridgeAccessList

>> management

cms2SessionCount
tftpSessionCount
cliSessionCount
tcpSessionCount

>> operatingSystem

currUsedProcPower
usedProcPower
freeDataBuffers
totalDataBuffers
largestFreeBlockSize
freeBlockCount
freeMemory
totalMemory
taskInfo

15.2 LAN interface performance attributes

This section describes the following performance attributes:

- telindus24xx/lanInterface/ifInOctets on page 586
- telindus24xx/lanInterface/ifInUcastPkts on page 586
- telindus24xx/lanInterface/ifInNUcastPkts on page 586
- telindus24xx/lanInterface/ifInDiscards on page 586
- telindus24xx/lanInterface/ifInErrors on page 586
- telindus24xx/lanInterface/ifInUnknownProtos on page 586
- telindus24xx/lanInterface/ifOutOctets on page 587
- telindus24xx/lanInterface/ifOutUcastPkts on page 587
- telindus24xx/lanInterface/ifOutNUcastPkts on page 587
- telindus24xx/lanInterface/ifOutDiscards on page 587
- telindus24xx/lanInterface/ifOutErrors on page 587
- telindus24xx/lanInterface/ifOutQLen on page 587
- telindus24xx/lanInterface/h2Performance on page 588
- telindus24xx/lanInterface/h24Performance on page 588

telindus24xx/lanInterface/ifInOctets

This attribute displays the number of octets (bytes) received on this interface.

telindus24xx/lanInterface/ifInUcastPkts

This attribute displays the number of unicast packets received on this interface and delivered to a higher-layer protocol. Unicast packets are all non-multicast and non-broadcast packets.

telindus24xx/lanInterface/ifInNUcastPkts

This attribute displays the number of non-unicast packets received on this interface and delivered to a higher-layer protocol. Non-unicast packets are all the multicast and broadcast packets.

telindus24xx/lanInterface/ifInDiscards

This attribute displays the number of incoming packets that were discarded, to prevent their deliverance to a higher-layer protocol. This even though no errors were detected in these packets.

telindus24xx/lanInterface/ifInErrors

This attribute displays the number of incoming packets that could not be delivered to a higher-layer protocol because they contained errors.

telindus24xx/lanInterface/ifInUnknownProtos

This attribute displays the number of incoming packets that were discarded because they contained an unknown or unsupported protocol.

telindus24xx/lanInterface/ifOutOctets

This attribute displays the total number of octets (bytes) transmitted by the interface, including framing characters.

telindus24xx/lanInterface/ifOutUcastPkts

This attribute displays the total number of packets that higher-level protocols requested to be transmitted to a unicast address, including those that were discarded or not sent.

telindus24xx/lanInterface/ifOutNUcastPkts

This attribute displays the number of non-unicast packets that higher-level protocols requested to be transmitted to a non-unicast (i.e. a broadcast or multicast) address, including those that were discarded or not sent.

telindus24xx/lanInterface/ifOutDiscards

This attribute displays the number of outgoing packets that were discarded, to prevent they are transmitted by the interface. This could be due to, for instance, the presence of an access list.

telindus24xx/lanInterface/ifOutErrors

This attribute displays the number of outgoing packets that could not be transmitted by the interface because they contained errors.

telindus24xx/lanInterface/ifOutQLen

This attribute displays the length, expressed in packets, of the output packet queue on the interface.

telindus24xx/lanInterface/h2Performance

This attribute displays the 2 hours performance summary of the LAN interface.

The h2Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
ifUpTime	the time during which the interface was up.
ifStatusChanges	the number of times the ifOperStatus value of the interface changed (from up to down or vice versa).
ifInOctets	the number of octets (bytes) received on this interface.
ifInPackets	the number of packets received on this interface.
ifInErrors	the number of packets received on this interface that could not be delivered to a higher-layer protocol because they contained errors.
ifOutOctets	the number of octets (bytes) transmitted by the interface, including framing characters.
ifOutPackets	the number of packets transmitted by the interface.
ifOutDiscards	the number of outgoing packets that were discarded, to prevent they were transmitted by the interface. This could be due to, for instance, the presence of an access list.
ifOutErrors	the number of packets that could not be transmitted by the interface because they contained errors.

telindus24xx/lanInterface/h24Performance

This attribute displays the 24 hours performance summary of the LAN interface. The h24Performance table contains the same elements as the telindus24xx/lanInterface/h2Performance table.

15.3 4 port Ethernet interface performance attributes

The performance attributes of the 4 port Ethernet interface are the same as those of the LAN interface. Refer to 15.2 - LAN interface performance attributes on page 585.

15.4 6E1 interface performance attributes

This section describes the following performance attributes:

- telindus24xx/hexE1/e1[E1_x]/h2G703Performance on page 591
- telindus24xx/hexE1/e1[E1_x]/h24G703Performance on page 591
- telindus24xx/hexE1/e1[E1_x]/d7G703Performance on page 591
- telindus24xx/hexE1/e1[E1_x]/g703Performance on page 591
- telindus24xx/hexE1/e1[E1_x]/h2G826Performance on page 592
- telindus24xx/hexE1/e1[E1_x]/h24G826Performance on page 592
- telindus24xx/hexE1/e1[E1_x]/d7G826Performance on page 592
- telindus24xx/hexE1/e1[E1_x]/g826Performance on page 592
- telindus24xx/hexE1/e1[E1_x]/tcPerformance on page 593

telindus24xx/hexE1/e1[E1_x]/h2G703Performance

This attribute displays the 2 hours performance summary of the E1 interface. The h2G703Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
losCount	the number of times a Loss Of Signal condition occurred.
losTime	the amount of time a Loss Of Signal condition was active.
aisCount	the number of times an Alarm Indication Signal condition occurred.
aisTime	the amount of time an Alarm Indication Signal condition was active.
lfaCount	the number of times a Loss of Frame Alignment condition occurred.
lfaTime	the amount of time a Loss of Frame Alignment condition was active.

telindus24xx/hexE1/e1[E1_x]/h24G703Performance

This attribute displays the 24 hours performance summary of the E1 interface. The h24G703Performance table contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G703Performance table.

telindus24xx/hexE1/e1[E1_x]/d7G703Performance

This attribute displays the 7 days performance summary of the E1 interface. The d7G703Performance table contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G703Performance table.

telindus24xx/hexE1/e1[E1_x]/g703Performance

This attribute displays the performance summary of the E1 interface since the last cold boot. Except for the sysUpTime, the g703Performance structure contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G703Performance table.

telindus24xx/hexE1/e1[E1_x]/h2G826Performance

This attribute displays the 2 hours G.826 performance summary of the E1 interface. The h2G826Performance table contains the following elements:

Element	For the corresponding period, this value displays …
sysUpTime	the elapsed time since the last cold boot.
errBlocks	the number of errored blocks that was counted.
errSec	the number of errored seconds that was counted.
sevErrSec	the number of severely errored seconds that was counted.
unavailCount	the number of times the interface was down (i.e. unavailable, as defined in ITU-T recommendation G.826 Annex A).
unavailTime	the amount of time the interface was down.
bBErrors	the number of background block errors that was counted.

Also see E1 interface performance definitions on page 594.

telindus24xx/hexE1/e1[E1_x]/h24G826Performance

This attribute displays the 24 hours G.826 performance summary of the E1 interface. The h24G826Performance table contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G826Performance table.

telindus24xx/hexE1/e1[E1_x]/d7G826Performance

This attribute displays the 7 days G.826 performance summary of the E1 interface. The d7G826Performance table contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G826Performance table.

telindus24xx/hexE1/e1[E1_x]/g826Performance

This attribute displays the G.826 performance summary of the E1 interface since the last cold boot. Except for the sysUpTime, the g826Performance structure contains the same elements as the telindus24xx/hexE1/e1[E1_x]/h2G826Performance table.

telindus24xx/hexE1/e1[E1_x]/tcPerformance

This attribute displays the performance information of the TC (Transmission Convergence) layer. The tcPerformance table contains the following elements:

Element	Description
rxCells	This element displays the amount of received, error-free cells.
txCells	This element displays the amount of transmitted cells.
errorCells	This element displays the amount of received cells that are discarded due to header errors.
correctedCells	This element displays the amount of received cells with HEC (Header Error Check) single bit error that are corrected.
txIdleCells	This element displays the amount of transmitted idle cells.
filteredCells	This element displays the amount of filtered (i.e. discarded) idle or unassigned cells.

E1 interface performance definitions

The following table lists some of the definitions that are used in the ITU-T recommendations that apply on the E1 interface. They are listed here for completeness only. For more detailed information, refer to the recommendations themselves.

Term	Definition
defect	A defect is one of the following conditions: • Loss Of Signal (LOS, defined in G.775). • Alarm Indication Signal (AIS, defined in G.775). • Loss of Frame Alignment (LFA, defined in G.706).
Errored Block (EB)	A data frame that contains one or more errors. In case of G.704 framing a frame is time slot 0 up to time slot 31.
Errored Second (ES)	A 1 second period where at least 1 EB or defect occurred.
Severely Errored Second (SES)	A 1 second period where equal to or more than 30% EBs occur or at least 1 defect. The measurement of EBs depends on the operation mode: • Framed without CRC-4: the error detection occurs based on the detected Frame Alignment Signal (FAS) bit errors; 28 FAS bit errors per second matches a Bit Error Rate (BER) of 10^{-3} or more. • Framed with CRC-4: the error detection occurs based on CRC-4.
unavailability	Matches a period of 10 or more consecutive SESs. Refer to G.826 Annex A for a complete definition.

15.5 E3/T3 interface performance attributes

This section discusses the performance attributes of the E3/T3 interface. First it describes the specific E3/T3 interface performance attributes. Then, it explains the ATM related performance attributes of the E3/T3 interface.

The following gives an overview of this section:

- 15.5.1 - Specific E3/T3 interface performance attributes on page 596
- 15.5.2 - ATM performance attributes on the E3/T3 interface on page 599

15.5.1 Specific E3/T3 interface performance attributes

This section describes the following performance attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/h2G703Performance on page 597
- telindus24xx/e3T3/e3T3[E3T3_x]/h24G703Performance on page 597
- telindus24xx/e3T3/e3T3[E3T3_x]/d7G703Performance on page 597
- telindus24xx/e3T3/e3T3[E3T3_x]/g703Performance on page 597
- telindus24xx/e3T3/e3T3[E3T3_x]/h2G826Performance on page 598
- telindus24xx/e3T3/e3T3[E3T3_x]/h24G826Performance on page 598
- telindus24xx/e3T3/e3T3[E3T3_x]/d7G826Performance on page 598
- telindus24xx/e3T3/e3T3[E3T3_x]/g826Performance on page 598

telindus24xx/e3T3/e3T3[E3T3_x]/h2G703Performance

This attribute displays the 2 hours performance summary of the E3/T3 interface. The h2G703Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
losCount	the number of times a Loss Of Signal condition occurred.
losTime	the amount of time a Loss Of Signal condition was active.
aisCount	the number of times an Alarm Indication Signal condition occurred.
aisTime	the amount of time an Alarm Indication Signal condition was active.
lfaCount	the number of times a Loss of Frame Alignment condition occurred.
lfaTime	the amount of time a Loss of Frame Alignment condition was active.

telindus24xx/e3T3/e3T3[E3T3_x]/h24G703Performance

This attribute displays the 24 hours performance summary of the E3/T3 interface. The h24G703Performance table contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G703Performance table.

telindus24xx/e3T3/e3T3[E3T3_x]/d7G703Performance

This attribute displays the 7 days performance summary of the E3/T3 interface. The d7G703Performance table contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G703Performance table.

telindus24xx/e3T3/e3T3[E3T3_x]/g703Performance

This attribute displays the performance summary of the E3/T3 interface since the last cold boot. Except for the sysUpTime, the g703Performance structure contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G703Performance table.

telindus24xx/e3T3/e3T3[E3T3_x]/h2G826Performance

This attribute displays the 2 hours G.826 performance summary of the E3/T3 interface. The h2G826Performance table contains the following elements:

Element	For the corresponding period, this value displays …
sysUpTime	the elapsed time since the last cold boot.
errBlocks	the number of errored blocks that was counted.
errSec	the number of errored seconds that was counted.
sevErrSec	the number of severely errored seconds that was counted.
unavailCount	the number of times the interface was down (i.e. unavailable, as defined in ITU-T recommendation G.826 Annex A).
unavailTime	the amount of time the interface was down.
bBErrors	the number of background block errors that was counted.

Also see E1 interface performance definitions on page 594.

telindus24xx/e3T3/e3T3[E3T3_x]/h24G826Performance

This attribute displays the 24 hours G.826 performance summary of the E3/T3 interface. The h24G826Performance table contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G826Performance table.

telindus24xx/e3T3/e3T3[E3T3_x]/d7G826Performance

This attribute displays the 7 days G.826 performance summary of the E3/T3 interface. The d7G826Performance table contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G826Performance table.

telindus24xx/e3T3/e3T3[E3T3_x]/g826Performance

This attribute displays the G.826 performance summary of the E3/T3 interface since the last cold boot. Except for the sysUpTime, the g826Performance structure contains the same elements as the telindus24xx/e3T3/e3T3[E3T3_x]/h2G826Performance table.

15.5.2 ATM performance attributes on the E3/T3 interface

This section describes the following performance attributes:

- telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc on page 600
- telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp on page 600
- telindus24xx/e3T3/e3T3[E3T3_x]/atm/unknownCells on page 600

telindus24xx/e3T3/e3T3[E3T3_x]/atm/pvc

This attribute gives the complete performance information of all the PVCs (Virtual Channels) that are present on the E3/T3 interface.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc for a detailed description of the pvc table.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/vp

This attribute lists the complete performance information of all the VPs (Virtual Channels) that are present on the xDSL interface.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp for a detailed description of the vp table.

telindus24xx/e3T3/e3T3[E3T3_x]/atm/unknownCells

This attribute displays the number of received cells for an unidentified PVC.

Example

Suppose router A sends OAM F4 loopback cells on VPI 5. On router B no VPI 5 is configured or no OAM F4 loopback cells are configured for VPI 5. In that case, the unknownCells value on router B will increase.

15.6 IMA group performance attributes

This section describes the following performance attributes:

- telindus24xx/bundle/imaGroup[ ]/pvc on page 602
- telindus24xx/bundle/imaGroup[ ]/members on page 602

telindus24xx/bundle/imaGroup[ ]/pvc

This attribute lists the complete performance information of all PVCs that are part of the IMA group.

Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc on page 614 for a detailed description of the pvc table.

telindus24xx/bundle/imaGroup[ ]/members

This attribute gives the complete performance information of all the members of the IMA group.

The members table contains the following elements:

Element	Description
interface	This element displays the name of the E1 interface that is a member of the IMA group.
id	This element displays the logical ID of the link on the E1 interface that makes up the IMA bundle.
rxTestPattern	This element displays the test pattern received in the ICP cells.
uniStatistics	This element displays the IMA User-Network Interface (UNI) statistics. The uniStatistics structure contains the following elements:

Element	Description
parityErrors	This displays the amount of discarded cells due to errors (parity, short or long cells).
misinsertedCells	This displays the amount of discarded cells due to address look-up failure.
crc10Failures	This displays the amount of discarded cells due to CRC 10 errors.

15.7 xDSL interface performance attributes

This section lists the performance attributes of the SHDSL and ADSL interfaces. With the exception of the actions retrain and testActivation, the performance attributes of the SHDSL and ADSL interfaces are the same. First this section lists the performance attributes of the line. Then it lists the performance attributes of the line pair.

- On a Telindus 2400 ADSL model, the line, linePair and end objects are always present. The repeater object does not exist on this model.
- On a Telindus 2400 SHDSL model, the line, linePair, repeater and end objects are added dynamically:
  - The line and linePair objects only appear when the necessary profiles have been configured and applied.
  - The repeater and end objects only appear when a connection with a repeater and/or remote SHDSL device has been established successfully.

The following gives an overview of this section:

- 15.7.1 - xDSL line performance attributes on page 604
- 15.7.2 - xDSL line pair performance attributes on page 610

15.7.1 xDSL line performance attributes

This section describes the following performance attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line on page 605
- telindus24xx/dslInterfaces/interface[dsl_x]/line/h24Line on page 605
- telindus24xx/dslInterfaces/interface[dsl_x]/line/d7Line on page 605
- telindus24xx/dslInterfaces/interface[dsl_x]/line/line on page 605

This section describes the following actions:

- telindus24xx/dslInterfaces/interface[dsl_x]/line/retrain on page 605

telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line

This attribute displays the 2 hours performance information summary of the line.

The h2Line table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
linkDownCount	the number of times the link went down.
linkDownTime	the total amount of time the link was down.

telindus24xx/dslInterfaces/interface[dsl_x]/line/h24Line

This attribute displays the 24 hours performance information summary of the line. The h24Line table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/d7Line

This attribute displays the 7 days performance information summary of the line. The d7Line table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/line

This attribute displays the performance information summary of the line since the last cold boot. Except for the sysUpTime, the line structure contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/retrain

This action is present on the Telindus 2400 SHDSL models only.

Use this action to force a retrain on the line.

15.7.2 xDSL line pair performance attributes

This section describes the following performance attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2LineParameters on page 611
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2Performance on page 611
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h24LineParameters on page 612
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h24Performance on page 612
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/d7LineParameters on page 612
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/d7Performance on page 612
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/lineParameters on page 612
- telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/performance on page 612

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2LineParameters

This attribute displays the 2 hours line parameter summary.

The h2LineParameters table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
lineAttenuationMin	the minimum line attenuation that was measured.
lineAttenuationAvrg	the average line attenuation that was calculated
lineAttenuationMax	the maximum line attenuation that was measured.
noiseMarginMin	the minimum noise margin that was measured.
noiseMarginAvrg	the average noise margin that was calculated.
noiseMarginMax	the maximum noise margin that was measured.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2Performance

This attribute displays the 2 hours performance summary of the line.

The h2Performance table contains the following elements:

Element	For the corresponding period, this element displays …
sysUpTime	the elapsed time since the last cold boot.
codeViolations	the number of line errors that was counted.
errSec	the number of erroneous seconds that was counted.
sevErrSec	the number of severely erroneous seconds that was counted.
unavailSec	the number of unavailable seconds that was counted.
loswSec	the number of lost synchronisation words seconds that was counted.
moniSec	the number of monitored seconds.

- Errors are counted based on the xDSL frame CRC.
- For the correct and unambiguous definition of code violations, errored and severely errored seconds, unavailability and lost synchronisation words seconds, refer to the recommendation G.826.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h24LineParameters

This attribute displays the 24 hours line parameter summary. The h24LineParameters table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2LineParameters table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h24Performance

This attribute displays the 24 hours performance summary of the line. The h24Performance table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2Performance table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/d7LineParameters

This attribute displays the 7 days line parameter summary. The d7LineParameters table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2LineParameters table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/d7Performance

This attribute displays the 7 days performance summary of the line. The d7Performance table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2Performance table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/lineParameters

This attribute displays the line parameter summary since the last cold boot. Except for the sysUpTime, the lineParameters table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2LineParameters table.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/performance

This attribute displays the performance summary of the line since the last cold boot. Except for the sysUpTime, the performance table contains the same elements as the telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair[ ]/h2Performance table.

15.8 ATM performance attributes

This section describes the following performance attributes:

- telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc on page 614
- telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp on page 616
- telindus24xx/dslInterfaces/interface[dsl_x]/atm/uniStatistics on page 616

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc

This attribute lists the complete performance information of all the PVCs (Virtual Channels) that are present on the xDSL interface.

The pvcTable table contains the following elements:

Element	Description
name	This is the name of the PVC as you configured it.
mibCounters	This displays the SNMP MIB2 parameters of the PVC. These are the same as the SNMP MIB2 parameters on the LAN interface. Refer to 15.2 - LAN interface performance attributes on page 585.
priorityQLengths	In case an overload condition occurs and priority queuing is activated, then this elements displays how many packets the different queues contain. Refer to 9.7.1 - Introducing traffic and priority policy on page 208 for more information on the priority queues.
atm	This displays the specific ATM related performance information of the PVC. Refer to telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm on page 615 for a detailed description of the atm structure

telindus24xx/dslInterfaces/interface[dsl_x]/atm/pvc/atm

The atm structure in the pvc table displays the specific ATM related performance information of the PVC.

The atm structure contains the following elements:

Element	Description
vpi	This displays the Virtual Path Identifier (VPI).
vci	This displays the Virtual Channel Identifier (VCI). The VPI in conjunction with the VCI identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination.
oamF5	This displays the performance information of the OAM F5 loop-back cells. The oamF5 structure contains the following elements: **Element** / **Description** rxLoopback — This displays the number of received OAM F5 loop-back cells. txLoopback — This displays the number of transmitted OAM F5 loop-back cells. rxAis — This displays the number of received OAM Alarm Indication Signals. txAis — This displays the number of transmitted OAM Alarm Indication Signals. rxRdi — This displays the number of received OAM Remote Defect Indications. txRdi — This displays the number of transmitted OAM Remote Defect Indications. **What is OAM AIS and RDI?** OAM PVC-AIS (Alarm Indication Signal) and PVC-RDI (Remote Defect Indication) are cells that are used for identifying and reporting PVC defects end-to-end. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream PVCs affected by the failure. Upon receiving an AIS cell on a PVC, the router marks the logical interface down and sends an RDI cell on the same PVC to let the remote end know the error status. When an RDI cell is received on a PVC, the router sets the logical interface status to down.

telindus24xx/dslInterfaces/interface[dsl_x]/atm/vp

This attribute lists the complete performance information of all the VPs (Virtual Channels) that are present on the xDSL interface.

The vp table contains the following elements:

Element	Description
vpi	This is the Virtual Path Identifier (VPI).
oamF4	This displays the performance information of the OAM F4 loop-back cells. The oamF4 structure contains the following elements:

Element	Description
rxLoopback	This displays the number of received OAM F4 loop-back cells.
txLoopback	This displays the number of transmitted OAM F4 loop-back cells.

telindus24xx/dslInterfaces/interface[dsl_x]/atm/uniStatistics

This attribute displays the ATM User-Network Interface (UNI) statistics.

The uniStatistics structure contains the following elements:

Element	Description
parityErrors	This displays the amount of discarded cells due to errors (parity, short or long cells).
misinsertedCells	This displays the amount of discarded cells due to misinserted cells. Misinserted cells are cells received for an unidentified PVC.
crc10Failures	This displays the amount of discarded cells due to CRC 10 errors.

15.9 Router performance attributes

This section discusses the performance attributes concerned with routing. First it describes the general routing performance attributes such as routingTable, etc. Then it explains the performance attributes of the extra features such as address translation, L2TP tunnelling, etc.

The following gives an overview of this section:

- 15.9.1 - General router performance attributes on page 618
- 15.9.2 - Default NAT performance attributes on page 622
- 15.9.3 - L2TP tunnel performance attributes on page 625
- 15.9.4 - Manual SA performance attributes on page 627

15.9.1 General router performance attributes

This section describes the following performance attributes:

- telindus24xx/ip/router/routingTable on page 619
- telindus24xx/ip/router/radiusAuth on page 620
- telindus24xx/ip/router/radiusAcct on page 620
- telindus24xx/ip/router/pingResults on page 621

This section describes the following actions:

- telindus24xx/ip/router/startPing on page 621
- telindus24xx/ip/router/stopPing on page 621

telindus24xx/ip/router/routingTable

This attribute lists all known routes and how many times they are used.

The routingTable contains the following elements:

Element	Description
network	This is the IP address of the destination network.
mask	This is the network mask of the destination network.
gateway	This is the IP address of the next router on the path to the destination network.
interface	This is the interface through which the destination network can be reached. Possible values are: **Value** / **Description** internal: The own protocol stack is used. <name>: The destination network can be reached through this particular interface. The <name> of the interface is the name as you configured it. Note that the “interface” can also be a DLCI, an ATM PVC, a tunnel, etc. discard: Packets for this destination are discarded.
uses	This lists how many times the route has been used since it is listed in the routing table. For each IP packet that matches this route, the attribute value is incremented by one. RIP routes may disappear from the routing table, and re-appear afterwards. The attribute value is reset when a RIP route disappears from the routing table.

telindus24xx/ip/router/radiusAuth

This attribute lists the RADIUS authentication server performance information.

The radiusAuth table contains the following elements:

Element	Description
server	This is the IP address of the authentication server.
requests	This is the number of access requests that is sent to the authentication server.
accepts	This is the number of access accepts that is received from the authentication server.
rejects	This is the number of access rejects that is received from the authentication server.
challenges	This is the number of access challenges that is received from the authentication server.
badAuthenticators	This is the total number of packets that contained invalid Message-Authenticator attributes.
timeOuts	This is the authentication time-out.
droppedPackets	This is the number of incoming packets dropped for reasons other than being malformed, bad authenticators, or unknown types.

telindus24xx/ip/router/radiusAcct

This attribute lists the RADIUS accounting server performance information.

The radiusAcct structure contains the following elements:

Element	Description
server	This is the IP address of the accounting server.
requests	This is the number of accounting requests that is sent to the accounting server.
responses	This is the number of accounting responses that is received from the accounting server.
badAuthenticators	This is the number of packets that contained invalid Signature attributes.
timeOuts	This is the accounting time-out.
droppedPackets	This is the number of incoming packets dropped for reasons other than being malformed, bad authenticators, or unknown types.

telindus24xx/ip/router/pingResults

You can use the startPing action to send a ping to an IP address (only one ping at a time). The pingResults attribute then lists the results of the transmitted ping.

The routingTable contains the following elements:

Element	Description
ipAddress	This is the IP address being pinged.
numOfTxPackets	This is the number of transmitted pings.
numOfRxPackets	This is the number of correct received answers on the transmitted pings.
minReplyTime	This is the lowest reply time of all correct received answers.
maxReplyTime	This is the highest reply time of all correct received answers.
avrgReplyTime	This is the average reply time of all correct received answers.

telindus24xx/ip/router/startPing

Execute this action to start transmitting pings to an IP address. Several arguments can be set:

Argument	Description
ipAddress	This is the IP address you want to ping. Default:0.0.0.0 Range: up to 255.255.255.255
iterations	This is the number of pings. If you enter 0, the IP address will be pinged an indefinite number of times. The only way to stop the ping session is by executing the stopPing action. Default:5 Range: 0 …
interval	This is the interval, in seconds, between consecutive pings. Default:1 Range: 0 … 100
dataLength	This is the length, in bytes, of the data transmitted in a ping. Default:31 Range: 0 … 1300
timeOut	If a ping is sent, the system will wait for a certain period on the answer. I.e. the system expects the answer within this period. Use the timeOut argument to set this period. Default:00000d 00h 00m 05s Range: 00000d 00h 00m 00s - 24855d 03h 14m 07s

telindus24xx/ip/router/stopPing

Execute this action to stop pending pings.

15.9.2 Default NAT performance attributes

This section describes the following performance attributes:

- telindus24xx/ip/router/defaultNat/socketsFree on page 623
- telindus24xx/ip/router/defaultNat/allocFails on page 623
- telindus24xx/ip/router/defaultNat/discards on page 623
- telindus24xx/ip/router/defaultNat/addressesAvailable on page 623
- telindus24xx/ip/router/defaultNat/tcpSocketsUsed on page 623
- telindus24xx/ip/router/defaultNat/udpSocketsUsed on page 623
- telindus24xx/ip/router/defaultNat/icmpSocketsUsed on page 623
- telindus24xx/ip/router/defaultNat/tcpAllocs on page 624
- telindus24xx/ip/router/defaultNat/udpAllocs on page 624
- telindus24xx/ip/router/defaultNat/icmpAllocs on page 624

This section describes the following actions:

- telindus24xx/ip/router/defaultNat/resetNat on page 624

telindus24xx/ip/router/defaultNat/socketsFree

This attribute shows the remaining number of new connections (i.e. sockets) that can be initiated. A socket is a set of source and destination IP addresses and port numbers.

Initially, 2048 simultaneous sockets can be initiated. Sockets are freed using a garbage mechanism. This means that every five minutes all sockets are checked. If a socket has been released by PAT or NAT, then this socket is returned to the pool of free sockets.

ICMP and UDP sockets are released when they have no data traffic during five minutes. TCP sockets are released after the TCP session has been closed or when the session has been idle for 24 hours.

telindus24xx/ip/router/defaultNat/allocFails

If no sockets are available anymore but an attempt to set up a new connection is being made, then the natAllocFails attribute value is incremented by 1.

Because the sockets are distributed using a hashing function, it is possible that natAllocFails increases even though natSocketsFree still indicates free sockets.

ICMP requires a new socket for each transmitted packet. This implies that, for instance, a permanent ping or trace-route command may eventually use all free sockets.

telindus24xx/ip/router/defaultNat/discards

This attribute indicates how many times a packet has been discarded for reasons other than a lack of free sockets. This could be, for instance, because an attempt was made to connect from the Internet to a service that was not present in the servicesAvailable table.

telindus24xx/ip/router/defaultNat/addressesAvailable

This attribute displays the number of NAT addresses that are currently free.

telindus24xx/ip/router/defaultNat/tcpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for TCP applications.

telindus24xx/ip/router/defaultNat/udpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for UDP applications.

telindus24xx/ip/router/defaultNat/icmpSocketsUsed

This attribute displays the number of sockets currently in use by PAT and NAT for ICMP applications.

telindus24xx/ip/router/defaultNat/tcpAllocs

This attribute indicates how many TCP sockets have been allocated since cold boot. Together with the performance attributes natUdpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

telindus24xx/ip/router/defaultNat/udpAllocs

This attribute indicates how many UDP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natIcmpAllocs it gives an indication of the type of traffic that is being routed.

telindus24xx/ip/router/defaultNat/icmpAllocs

This attribute indicates how many ICMP sockets have been allocated since cold boot. Together with the performance attributes natTcpAllocs and natUdpAllocs it gives an indication of the type of traffic that is being routed.

telindus24xx/ip/router/defaultNat/resetNat

Use this action to release all sockets currently in use and return them to the free socket pool.

In other words, executing this action resets all NAT/PAT sessions that are currently established. It also releases all official IP addresses that are dynamically assigned to a private IP address. If any TCP sessions are still active, these sessions will be aborted.

Take care when using this action! All TCP information is lost when the sockets are released with this action. Any TCP sessions in use at the time of the reset will go into a hang-up state. These applications will need to restart.

15.9.3 L2TP tunnel performance attributes

This section describes the following performance attributes:

- telindus24xx/ip/router/tunnels/l2tpTunnels on page 626
- telindus24xx/ip/router/tunnels/ipsecL2tpTunnels on page 626

telindus24xx/ip/router/tunnels/l2tpTunnels

This attribute displays the performance information of the L2TP tunnels.

The l2tpTunnels table contains the following elements:

Element	Description
name	This is the name of the tunnel as you configured it.
mibCounters	This displays the SNMP MIB2 parameters of the tunnel. These are the same as the SNMP MIB2 parameters on the LAN interface. Refer to 15.2 - LAN interface performance attributes on page 585.

telindus24xx/ip/router/tunnels/ipsecL2tpTunnels

This attribute displays the performance information of the L2TP tunnels.

The ipsecL2tpTunnels table contains the same elements as the l2tpTunnels table. Refer to telindus24xx/ip/router/tunnels/l2tpTunnels on page 626.

15.9.4 Manual SA performance attributes

This section describes the following performance attributes:

- telindus24xx/ip/router/manualSA[ ]/inPackets on page 628
- telindus24xx/ip/router/manualSA[ ]/outPackets on page 628
- telindus24xx/ip/router/manualSA[ ]/espDecryptionFailure on page 628
- telindus24xx/ip/router/manualSA[ ]/espAuthenticationFailure on page 628
- telindus24xx/ip/router/manualSA[ ]/espSequenceNrReplay on page 628
- telindus24xx/ip/router/manualSA[ ]/espDroppedFrames on page 628

telindus24xx/ip/router/manualSA[ ]/inPackets

Upon receipt of a (reassembled) packet containing an ESP Header, the receiver determines the appropriate SA, based on the destination IP address, security protocol (ESP), and the SPI. Once the appropriate SA is determined, the inPackets attribute is incremented for this SA.

telindus24xx/ip/router/manualSA[ ]/outPackets

ESP is applied to an outbound packet only after it is determined that the packet is associated with an SA that calls for ESP processing. Once the appropriate SA is determined, the outPackets attribute is incremented for this SA.

telindus24xx/ip/router/manualSA[ ]/espDecryptionFailure

This attribute displays the number of times the decryption of an incoming ESP packet failed.

telindus24xx/ip/router/manualSA[ ]/espAuthenticationFailure

This attribute displays the number of times the authentication of an incoming ESP packet failed.

telindus24xx/ip/router/manualSA[ ]/espSequenceNrReplay

For each incoming ESP packet, the receiver verifies that the packet contains a sequence number that does not duplicate the sequence number of any other packets received during the life of this SA. Should this be the case, then these packets are dropped and the espSequenceNrReplay attribute is incremented for this SA.

telindus24xx/ip/router/manualSA[ ]/espDroppedFrames

This attribute displays the number of ESP packets that were successfully decrypted and authenticated, but that could not be delivered to the L2TP tunnel (e.g. because the tunnel was down) and had to be dropped.

15.10 Bridge performance attributes

This section discusses the performance attributes concerned with bridging. First it describes the general bridging performance attributes such as bridgeCache, etc. Then it explains the performance attributes of the extra features such as bridge access lists, etc…

The following gives an overview of this section:

- 15.10.1 - Bridge group performance attributes on page 630
- 15.10.2 - Bridge access list performance attributes on page 632

15.10.1 Bridge group performance attributes

This section describes the following performance attributes:

- telindus24xx/bridge/bridgeGroup/bridgeCache on page 631
- telindus24xx/bridge/bridgeGroup/bridgeDiscards on page 631
- telindus24xx/bridge/bridgeGroup/bridgeFloods on page 631

telindus24xx/bridge/bridgeGroup/bridgeCache

When a port of the bridge enters the learning state, it stores the MAC addresses of the stations situated on the network that is connected to this port. The MAC addresses are stored in a MAC address database or bridge cache. The bridgeCache attribute visualises this address database. Refer to What is the bridge cache? on page 448 for more information.

The bridgeCache table contains the following elements:

Element	Description
interface	This is the interface through which the station can be reached.
macAddress	This is the MAC address of the station situated on the network connected to the interface.
rxCount	This is the number of frames received from the corresponding MAC address.
txCount	This is the number of frames forwarded to the corresponding MAC address.

telindus24xx/bridge/bridgeGroup/bridgeDiscards

This attribute displays the number of times a frame was discarded because …

- it was received on the same interface as the one through which the destination address can be reached.
- it was received on an interface that is not in the forwarding state.

telindus24xx/bridge/bridgeGroup/bridgeFloods

This attribute displays the number of times a frame was flooded on all interfaces because …

- it was a broadcast / multicast.
- the position of the station with the destination MAC address was not known (yet).

15.10.2 Bridge access list performance attributes

This section describes the following performance attributes:

- telindus24xx/bridge/accessList[ ]/bridgeAccessList on page 633

telindus24xx/bridge/accessList[ ]/bridgeAccessList

This attribute shows information on the use of the bridge access list.

The bridgeAccessList table contains the following elements:

Element	Description
macAddress	This is the MAC address as configured in the configuration attribute telindus24xx/bridge/accessList[ ]/bridgeAccessList.
uses	This indicates the number of times a packet has been discarded for the corresponding MAC address.

15.11 Management performance attributes

This section describes the following performance attributes:

- telindus24xx/management/cms2SessionCount on page 635
- telindus24xx/management/cliSessionCount on page 635
- telindus24xx/management/tftpSessionCount on page 636
- telindus24xx/management/tcpSessionCount on page 636

telindus24xx/management/cms2SessionCount

This attribute displays the number of CMS2 sessions that are currently active on the Telindus 2400.

There are always minimum two fixed sessions active. Connecting with TMA, TMA CLI, Telnet, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for SNMP.
1 fixed session	A fixed session for O10.
+ 2 sessions	When connecting with TMA.
+ 1 session	When connecting with the Element Manager (which is a part of TMA Element Management and TMA for HP OpenView).
+ 1 session	When connecting with TMA CLI.
+ 2 sessions	When downloading a *config.cli* or *config.cms* file.
+ 1 session	When connecting with Telnet.
+ 1 session	When downloading software.
+ 1 session	When connecting with the Web Interface.

telindus24xx/management/cliSessionCount

This attribute displays the number of CLI sessions that are currently active on the Telindus 2400.

There are always minimum two fixed sessions active. Connecting with TMA CLI, the Web Interface, etc. opens additional sessions. This is explained in the following table:

Session count	Purpose
1 fixed session	A fixed session for the control port.
1 fixed session	A fixed session for Web Interface.
+ 1 session	When connecting with TMA CLI or starting a CLI session.
+ 1 session	When connecting with the Web Interface.

telindus24xx/management/tftpSessionCount

This attribute displays the number of TFTP sessions that are currently active on the Telindus 2400.

telindus24xx/management/tcpSessionCount

This attribute displays the number of TCP sessions that are currently active on the Telindus 2400. The following table shows when a TCP session opens:

Session count	Purpose
+ 1 session	When connecting with Telnet.
+ 1 session	When connecting with the Web Interface.

15.12 Operating system performance attributes

This section describes the following performance attributes:

- telindus24xx/operatingSystem/currUsedProcPower on page 638
- telindus24xx/operatingSystem/usedProcPower on page 638
- telindus24xx/operatingSystem/freeDataBuffers on page 638
- telindus24xx/operatingSystem/totalDataBuffers on page 638
- telindus24xx/operatingSystem/largestFreeBlockSize on page 638
- telindus24xx/operatingSystem/freeBlockCount on page 638
- telindus24xx/operatingSystem/freeMemory on page 639
- telindus24xx/operatingSystem/totalMemory on page 639
- telindus24xx/operatingSystem/taskInfo on page 639

telindus24xx/operatingSystem/currUsedProcPower

This attribute displays the amount of processing power used during the last 650 milliseconds, expressed as a percentage of the total available processing power.

telindus24xx/operatingSystem/usedProcPower

This attribute lists the used processing power for the 11 most recent 30 seconds intervals. The processing power is expressed as a percentage of the total processing power.

The usedProcPower table contains the following elements:

Element	Description
sysUpTime	This is the elapsed time since the last cold boot. The next values are for the 30 seconds period before this relative time stamp.
min	This is the minimum percentage of processing power in use during the last 30 seconds.
average	This is the average percentage of processing power in use during the last 30 seconds.
max	This is the maximum percentage of processing power in use during the last 30 seconds.

telindus24xx/operatingSystem/freeDataBuffers

The processor uses buffers for storing the packets during processing and/or queuing. Each buffer has a 256 byte size, headers included. This attribute is the number of data buffers currently not in use and available for e.g. incoming data.

telindus24xx/operatingSystem/totalDataBuffers

This attribute displays the total number of available data buffers.

telindus24xx/operatingSystem/largestFreeBlockSize

The processor uses RAM memory for storing internal information and buffering. The different tasks allocate RAM memory on request. Tasks may also free memory again. In this way the total RAM memory becomes fragmented. This attribute gives the size of the largest contiguous free memory block expressed in bytes.

telindus24xx/operatingSystem/freeBlockCount

This attribute displays the number of free contiguous memory blocks.

telindus24xx/operatingSystem/freeMemory

This attribute displays the total free memory expressed in bytes.

telindus24xx/operatingSystem/totalMemory

This attribute displays the total RAM memory expressed in bytes.

telindus24xx/operatingSystem/taskInfo

This attribute contains status information concerning the different tasks running on the processor. It is a table grouping up to 31 task slots, which is the maximum number of parallel tasks running on the processor's operating system.

This attribute contains the same elements as the status attribute telindus24xx/operatingSystem/taskInfo on page 577.

16 Alarm attributes

This chapter discusses the alarm attributes of the Telindus 2400. The following gives an overview of this chapter:

- 16.1 - Alarm attributes overview on page 642
- 16.2 - Introducing the alarm attributes on page 645
- 16.3 - General alarms on page 649
- 16.4 - LAN interface alarms on page 651
- 16.5 - 4 port Ethernet interface alarms on page 652
- 16.6 - 6E1 interface alarms on page 653
- 16.7 - E3/T3 interface alarms on page 654
- 16.8 - xDSL interface alarms on page 655
- 16.9 - Router alarms on page 662
- 16.10 - Alarm in contacts alarms on page 663

16.1 Alarm attributes overview

> telindus24xx
- totalAlarmLevel
- alarmInfo
  - notResponding
  - alarmSyncLoss
  - configChanged
  - access
  - powerSupply1Fail
  - powerSupply2Fail
  - overheating
  - unknownStatus
  - coldBoot
  - warmBoot
  - codeConsistencyFail
  - configConsistencyFail

>> lanInterface
- alarmInfo
  - linkDown

>> 4pEth
- alarmInfo
  - linkDown

>> hexE1

>>> e1[E1_x]
- alarmInfo
  - linkDown
  - lfa
  - ais
  - rai
  - sq

>> e3T3

>>> e3T3[E3T3_x]
- alarmInfo
  - linkDown
  - lfa
  - ais
  - rai
  - sq

>> dslInterfaces

>>> interface[dsl_x]
alarmInfo
linkDown

>>>> line
alarmInfo
linkDown

>>>>> linePair
alarmInfo
linkDown
lineAttenuation
noiseMargin
errSecExceeded
sevErrSecExceeded
remotePowerFail

>>>> repeater[1]

>>>>> networkLinePair
alarmInfo
lineAttenuation
noiseMargin
errSecExceeded
sevErrSecExceeded

>>>>> customerLinePair
alarmInfo
lineAttenuation
noiseMargin
errSecExceeded
sevErrSecExceeded

>>>> end

>>>>> linePair
alarmInfo
lineAttenuation
noiseMargin
errSecExceeded
sevErrSecExceeded

1. Telindus 2400 SHDSL models only (2421, 2422, 2423).

>> ip

>>> router

alarmInfo

pingActive

>> alarmContacts

alarmInfo

contactIn1

contactIn2

contactIn3

contactIn4

contactIn5

contactIn6

contactIn7

16.2 Introducing the alarm attributes

Before discussing the alarm attributes of the Telindus 2400 in detail, some general information on the alarm attributes of the Telindus 2400 is given.

The following gives an overview of this chapter:

- 16.2.1 - Alarm configuration attributes on page 646
- 16.2.2 - General alarm attributes on page 648

16.2.1 Alarm configuration attributes

This section describes the following alarm attributes:

- telindus24xx/…/alarmMask
- telindus24xx/…/alarmLevel
- telindus24xx/…/alarmContactHighMask on page 647
- telindus24xx/…/alarmContactLowMask on page 647

telindus24xx/…/alarmMask

Use this attribute to mask or unmask the alarms of an object. This determines whether an active alarm is sent to the central management system (e.g. HP OpenView) or not.

The alarms in the alarmMask attribute have the following values:

Value	Is the active alarm sent to the central management system?
enabled	Yes. So the alarm is *unmasked*.
disabled	No. So the alarm is *masked*.

Alarms are always seen in the alarmInfo alarm attribute of an object, regardless of the masking of the alarm. I.e. even if an alarm is set to disabled in the alarmMask of an object, if the alarm condition is fulfilled then the alarm will be set to on in the alarmInfo of that object. However, because this alarm is disabled it will not be sent to the central management system (e.g. HP OpenView).

Only the most important alarms are unmasked (i.e. enabled) by default. All other alarms are masked (i.e. disabled).

telindus24xx/…/alarmLevel

Use this attribute to assign a priority level to each alarm of the corresponding object. The alarm level range goes from 0 to 254, where 0 is the lowest and 254 is the highest priority level.

The alarmLevel of an unmasked, active alarm is sent to the totalAlarmLevel alarm attribute of the top object telindus24xx.

telindus24xx/.../alarmContactHighMask

Use this attribute to mask or unmask the alarms of an object. This determines whether an active alarm activates the high alarm contact or not. By connecting an alarm circuit to the alarm contact, e.g. a light bulb or a buzzer, you can generate an external alarm.

The alarms in the alarmContactHighMask attribute have the following values:

Value	Does the active alarm activate the high alarm contact?
enabled	Yes. So the alarm is *unmasked*.
disabled	No. So the alarm is *masked*.

All alarms are masked (i.e. disabled) by default.

telindus24xx/.../alarmContactLowMask

Use this attribute to mask or unmask the alarms of an object. This determines whether an active alarm activates the low alarm contact or not. By connecting an alarm circuit to the alarm contact, e.g. a light bulb or a buzzer, you can generate an external alarm.

The alarms in the alarmContactLowMask attribute have the following values:

Value	Does the active alarm activate the low alarm contact?
enabled	Yes. So the alarm is *unmasked*.
disabled	No. So the alarm is *masked*.

All alarms are masked (i.e. disabled) by default.

16.2.2 General alarm attributes

This section describes the following alarm attributes:

- telindus24xx/totalAlarmLevel
- telindus24xx/…/alarmInfo

telindus24xx/totalAlarmLevel

This attribute is only present in the top object of the containment tree of the Telindus 2400, being telindus24xx.

It displays the priority level of an unmasked, active alarm. When several alarms are generated at the same time, the highest priority level is shown. If the alarm levels are set in a structured manner, one look at the totalAlarmLevel attribute enables the operator to make a quick estimation of the problem.

The value of the totalAlarmLevel attribute is also communicated to the central management system (e.g. HP OpenView) where it determines the colour of the icon. This colour is an indication of the severity of the alarm.

telindus24xx/…/alarmInfo

This attribute contains the actual alarm information of the corresponding object.

The alarmInfo structure contains the following elements:

Element	This element displays for the corresponding object …
discriminator	the total alarm count since the last cold boot.
currentAlarms	the current alarms.
previousAlarms	the second most recent alarms.
alarmMask	the alarmMask as you configured it.
alarmLevel	the alarmLevel as you configured it.

16.3 General alarms

This section describes the alarms of the alarm attribute telindus24xx/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/alarmInfo

The different alarms related to the telindus24xx object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
notResponding	by the management concentrator when the Telindus 2400 does not respond on its polling session.	enabled	4
alarmSyncLoss	when the internal alarm buffer overflows.	enabled	4
configChanged	when the local configuration has been changed.	disabled	1
access	when a management session is started on the Telindus 2400 itself. This alarm is not activated when the management session is established through a management concentrator. **Example** The alarm is *activated* in case of … • a TMA, TMA CLI, terminal (CLI or ATWIN) or Easy-Connect session via the control connector of the Telindus 2400. • a TMA, TMA CLI, TMA Element Management, TMA for HP OpenView, Telnet (CLI or ATWIN), HTTP (Web Interface) or TFTP session using the LAN / WAN IP address of the Telindus 2400. The alarm is *not activated* in case of … • any management session (TMA, terminal, Telnet, HTTP, etc.) established *through a management concentrator* on the Telindus 2400. • SNMP management.	disabled	1
powerSupply1Fail	when the power supply connected to the upper power supply connector fails or is disconnected.	disabled	3
powerSupply2Fail	when the power supply connected to the lower power supply connector fails or is disconnected.	disabled	3
overheating	when the temperature inside the housing is too high.	enabled	3

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
unknownState	each time a new Telindus 2400 is added to the network and before the management concentrator has completed a first successful polling session.	disabled	0
coldBoot	each time the Telindus 2400 performs a cold boot.	disabled	1
warmBoot	each time the Telindus 2400 performs a warm boot.	disabled	1
codeConsistency-Fail	when the software consistency imposed by the management concentrator on the Telindus 2400 fails. For example, because of a loss of contact. In the management concentrator that manages the Telindus 2400 (e.g. the Orchid 1003 LAN, Telindus 1035 Orchid, etc.), check the status attribute nmsgroup/softConsistencyStatus to determine the problem.	disabled	1
configConsistency-Fail	when the configuration consistency imposed by the management concentrator on the Telindus 2400 fails. For example, because of a loss of contact. In the management concentrator that manages the Telindus 2400 (e.g. the Orchid 1003 LAN, Telindus 1035 Orchid, etc.), check the status attribute status attributes nmsgroup/objectTable/configState and configDiag to determine the problem.	disabled	1

16.4 LAN interface alarms

This section describes the alarms of the alarm attribute telindus24xx/lanInterface/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/lanInterface/alarmInfo

The alarm related to the lanInterface object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when no valid LAN data is detected. I.e. when the connection between the interface and the LAN is down.	enabled	3

16.5 4 port Ethernet interface alarms

This section describes the alarms of the alarm attribute telindus24xx/4pEth/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/4pEth/alarmInfo

The alarm related to the 4pEth object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when no valid Ethernet data is detected. I.e. when the connection between the interface and the Ethernet is down.	enabled	3

16.6 6E1 interface alarms

This section describes the alarms of the alarm attribute telindus24xx/hexE1/e1[E1_x]/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/hexE1/e1[E1_x]/alarmInfo

The alarms related to the e1[E1_x] object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when the incoming data is no longer present.	disabled	3
ais	when the AIS signal (also called *all ones*) is detected on the incoming data. AIS means there is an alarm occurring on the line upstream from the equipment that is connected to the E1 interface.	disabled	2
lfa	when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period. This alarm is also generated when the crc4Insertion attribute is set to enabled, but no CRC is present in the incoming data.	disabled	2
rai	when an RAI signal is detected on the incoming data. An RAI means the far-end equipment has a problem with the signal it is receiving from the local equipment.	disabled	2
sq	when the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime. For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated. For more information, refer to … • telindus24xx/hexE1/e1[E1_x]/sqThreshold • telindus24xx/hexE1/e1[E1_x]/sqTime	disabled	2

16.7 E3/T3 interface alarms

This section describes the alarms of the alarm attribute telindus24xx/e3T3/e3T3[E3T3_x]/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/e3T3/e3T3[E3T3_x]/alarmInfo

The alarms related to the e3T3[E3T3_x] object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when the incoming data is no longer present.	disabled	3
ais	when the AIS signal (also called *all ones*) is detected on the incoming data. AIS means there is an alarm occurring on the line upstream from the equipment that is connected to the E1 interface.	disabled	2
lfa	when the Frame Alignment Signal (FAS), which is present in time slot 0 of the G.704 framed data, is not detected after a certain period. This alarm is also generated when the crc4Insertion attribute is set to enabled, but no CRC is present in the incoming data.	disabled	2
rai	when an RAI signal is detected on the incoming data. An RAI means the far-end equipment has a problem with the signal it is receiving from the local equipment.	disabled	2
sq	when the sqThreshold value, i.e. the number of erroneous seconds, is exceeded within the sqTime. For example, if 10 (default) or more erroneous seconds occur within 1 minute (default), then a signal quality alarm is generated. For more information, refer to … • telindus24xx/e3T3/e3T3[E3T3_x]/sqThreshold • telindus24xx/e3T3/e3T3[E3T3_x]/sqTime	disabled	2

16.8 xDSL interface alarms

This section lists the alarms of the SHDSL and ADSL interfaces. First this section lists the general xDSL interface alarms. Then it lists the alarms of the line, followed by the alarms of the line pair and finally the alarms of the repeater and end device.

- On a Telindus 2400 ADSL model, the line, linePair and end objects are always present. The repeater object does not exist on this model.
- On a Telindus 2400 SHDSL model, the line, linePair, repeater and end objects are added dynamically:
  - The line and linePair objects only appear when the necessary profiles have been configured and applied.
  - The repeater and end objects only appear when a connection with a repeater and/or remote SHDSL device has been established successfully.

The following gives an overview of this section:

- 16.8.1 - General xDSL interface alarms on page 656
- 16.8.2 - xDSL line alarms on page 657
- 16.8.3 - xDSL line pair alarms on page 658
- 16.8.4 - xDSL repeater and end alarms on page 660

16.8.1 General xDSL interface alarms

This section describes the alarms of the alarm attribute telindus24xx/dslInterfaces/interface[dsl_x]/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/dslInterfaces/interface[dsl_x]/alarmInfo

The alarm related to the interface[dsl_x] object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when … • an erroneous situation has been detected in the encapsulation protocol (ATM or PPP). E.g a failed PPP authentication, an ATM PVC which is down, etc. • the line is not in data state. • the bit pump is not synchronised.	enabled	3

16.8.2 xDSL line alarms

This section describes the alarms of the alarm attribute telindus24xx/dslInterfaces/interface[dsl_x]/line/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/dslInterfaces/interface[dsl_x]/line/alarmInfo

The alarm related to the line object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when the line is down. I.e. no data can be transmitted over the line.	enabled	3

16.8.3 xDSL line pair alarms

This section describes the alarms of the alarm attribute telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/dslInterfaces/interface[dsl_x]/line/linePair/alarmInfo

The alarms related to the linePair object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
linkDown	when the line pair is down. I.e. no data can be transmitted over the line pair.	disabled	3
lineAttenuation	when the line attenuation exceeds the value configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds for at least 10 seconds. The alarm is cleared when the line attenuation drops below this value for at least 10 seconds. Note that the Telindus 2400 forces the remote xDSL device to use the linkAlarmThresholds/lineAttenuation as configured on the Telindus 2400. Refer to The eocHandling attribute (fixed to alarmConfiguration) on page 102.	disabled	1
noiseMargin	when the noise margin exceeds the value configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds for at least 10 seconds. The alarm is cleared when the noise margin drops below this value for at least 10 seconds. Note that the Telindus 2400 forces the remote xDSL device to use the linkAlarmThresholds/noiseMargin as configured on the Telindus 2400. Refer to The eocHandling attribute (fixed to alarmConfiguration) on page 102.	disabled	1
errSecExceeded	when the amount of erroneous seconds exceeds the value configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds within a 15 minutes period[1]. The alarm is cleared when the amount of erroneous seconds drops below this value within a 15 minutes period.	disabled	1

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
sevErrSecExceeded	when the amount of severely erroneous seconds exceeds the value configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds within a 15 minutes period[1]. The alarm is cleared when the amount of severely erroneous seconds drops below this value within a 15 minutes period.	disabled	2
remotePowerFail	when the remote xDSL device experiences a power failure.	disabled	1

1. The 15 minutes periods run synchronous with the 15 minutes periods of the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line performance attribute.
   Because alarms are raised or cleared within 15 minutes periods, there is a delay in the alarm status. For example, suppose that in the first minute of a 15 minutes period the errSecOn value is exceeded, then the errSecExceeded alarm is raised. The alarm stays on for the remainder of the 15 minutes period. The alarm is only cleared if also in the next 15 minutes period the errSecOn value is not exceeded.

16.8.4 xDSL repeater and end alarms

This section describes the alarms of the alarm attribute telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/alarmInfo.

- On a Telindus 2400 ADSL model, the line, linePair and end objects are always present. The repeater object does not exist on this model.
- On a Telindus 2400 SHDSL model, the line, linePair, repeater and end objects are added dynamically:
  - The line and linePair objects only appear when the necessary profiles have been configured and applied.
  - The repeater and end objects only appear when a connection with a repeater and/or remote SHDSL device has been established successfully.
    The repeater and end objects contain the same attributes, therefore only the alarms of the end object are described.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/dslInterfaces/interface[dsl_x]/end/linePair/alarmInfo

The alarms related to the end/linePair object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
lineAttenuation	when the line attenuation on the remote xDSL device exceeds the lineAttenuation value as it is configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds *of the Telindus 2400* for at least 10 seconds. The alarm is cleared when the line attenuation drops below this value for at least 10 seconds.	disabled	1
noiseMargin	when the noise margin on the remote xDSL device exceeds the noiseMargin value as it is configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds *of the Telindus 2400* for at least 10 seconds. The alarm is cleared when the noise margin drops below this value for at least 10 seconds.	disabled	1

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
errSecExceeded	when the amount of erroneous seconds on the remote xDSL device exceeds the errSecOn value as it is configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds *of the Telindus 2400* within a 15 minutes period[1]. The alarm is cleared when the amount of erroneous seconds drops below this value within a 15 minutes period.	disabled	1
sevErrSecExceeded	when the amount of severely erroneous seconds on the remote xDSL device exceeds the sevErrSecOn value as it is configured in the telindus24xx/profiles/xdsl/shdsl_default/linkAlarmThresholds *of the Telindus 2400* within a 15 minutes period[1]. The alarm is cleared when the amount of severely erroneous seconds drops below this value within a 15 minutes period.	disabled	2

1. The 15 minutes periods run synchronous with the 15 minutes periods of the telindus24xx/dslInterfaces/interface[dsl_x]/line/h2Line performance attribute.
   Because alarms are raised or cleared within 15 minutes periods, there is a delay in the alarm status. For example, suppose that in the first minute of a 15 minutes period the errSecOn value is exceeded, then the errSecExceeded alarm is raised. The alarm stays on for the remainder of the 15 minutes period. The alarm is only cleared if also in the next 15 minutes period the errSecOn value is not exceeded.

16.9 Router alarms

This section describes the alarms of the alarm attribute telindus24xx/ip/router/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/ip/router/alarmInfo

The alarm related to the router object together with its explanation and default alarmMask and alarmLevel value is given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
pingActive	when a ping is pending (for example, an indefinite ping). This notification is necessary because you can only transmit one ping at a time. Furthermore, there is no protection when a new ping is started before the previous is stopped.	enabled	3

16.10 Alarm in contacts alarms

This section describes the alarms of the alarm attribute telindus24xx/alarmContacts/alarmInfo.

Refer to 16.2 - Introducing the alarm attributes on page 645 for general information on the alarm attributes.

telindus24xx/alarmContacts/alarmInfo

The alarms related to the alarmContacts object together with their explanation and default alarmMask and alarmLevel value are given in the following table:

The alarm …	is generated …	Default value	
		alarmMask	alarmLevel
alarmIn1 ... alarmIn7	when a connection is made between pin 8 and respectively pin 1 up to 7 of the ALARM IN connector of the Telindus 2400. Refer to 13.14 - Alarm in contacts configuration attributes on page 456 for more information.	disabled	2

17 TMA sub-system picture

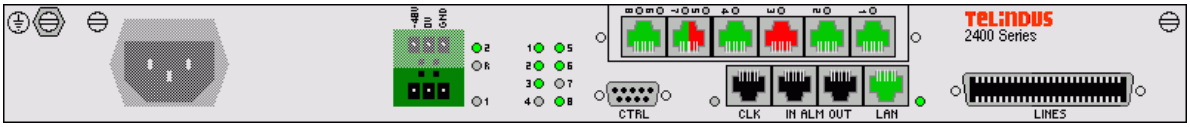
The sub-system picture is a TMA tool that visualises the status information of the Telindus 2400. This chapter explains how to display the sub-system picture, and how to interpret the visual indications.

How to display the sub-system picture?

To display the sub-system picture of the Telindus 2400, click on the sub-system picture button located in the TMA toolbar: .

Structure of the sub-system picture

This paragraph displays and labels the different elements of the sub-system picture. It also explains how the visual indications should be interpreted. Below, the Telindus 2400 sub-system picture is displayed:



The following table gives an overview of the sub-system picture elements and what they indicate:

Element	Description
LEDs	These reflect the actual status of the device. The LED indication on the sub-system picture corresponds with the LED indication on the Telindus 2400 itself. Refer to 2.7 - The front panel LED indicators on page 33 for more information on the interpretation of the LEDs.
interfaces	This reflects the status of the interfaces. The possible indications are: **Colour** / **Explanation** green: There is no alarm active in the corresponding interface object. red: An alarm is active in the corresponding interface object. The colours of the interfaces only change if the alarms related to the interface object are set to *enabled* in the alarmMask.

18 Auto installing the Telindus 2400

Auto install includes a number of features that allow you to partially or completely configure the Telindus 2400 without on-site intervention.

The following gives an overview of this chapter:

- 18.1 - Automatically obtaining an IP address using BootP or DHCP on page 668
- 18.2 - Automatically obtaining an IP address on the LAN on page 669
- 18.3 - Obtaining the configuration with TFTP on page 670
- 18.4 - Creating configuration files on page 673
- 18.5 - Creating a binary configuration file on page 674
- 18.6 - Creating an ASCII configuration file on page 675

18.1 Automatically obtaining an IP address using BootP or DHCP

The Telindus 2400 uses BootP and DHCP requests to obtain an IP address on its LAN interface. BootP and DHCP are very similar protocols. In both protocols, the client IP device sends a limited broadcast request on its interfaces requesting an IP address. The request contains the client its MAC address, which is a unique identifier.

The Telindus 2400, being a router, always requests a static IP address.

How works BootP?

A workstation with a BootP server interprets incoming BootP requests. You can configure a file on the server with MAC address and IP address/subnet mask pairs for all devices in the network you want to service. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask.

Assigning an IP address in this way is done through a simple request - response handshake.

How works DHCP?

A workstation with a DHCP server works in a similar way as with a BootP server. The difference with BootP is that you can additionally configure a list of IP addresses on the server. These IP addresses are dynamically assigned to the IP devices requesting an IP address, independently of their MAC address. Those address assignments are limited in time.

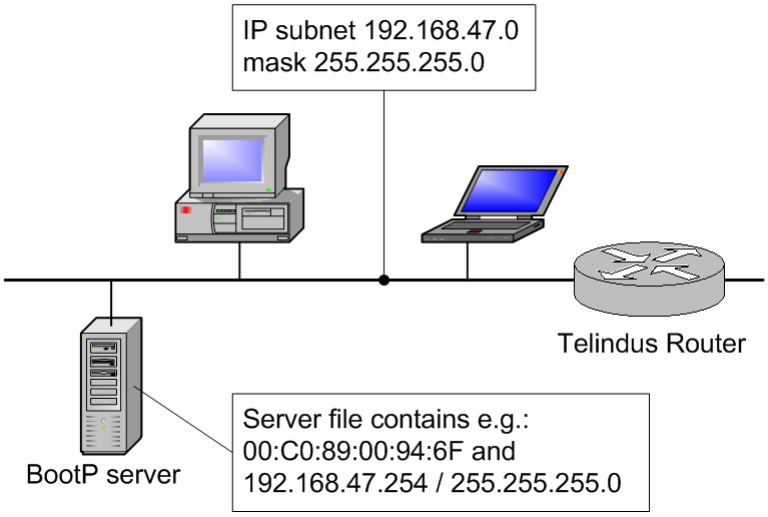
Assigning an IP address in this way is done through a 4-way handshake and with regular renewals.

The Telindus 2400 as BootP and DHCP relay agent

Being broadcast packets, BootP and DHCP requests can cross a router using IP helper addresses. The Telindus 2400 is a BootP and DHCP relay agent. This means it adds additional information to the request packets allowing servers on distant networks to send back the answer. This feature is not used in the auto install procedure.

18.2 Automatically obtaining an IP address on the LAN

The following figure shows how the Telindus 2400 obtains its LAN IP address from a BootP server on its Ethernet interface:



The IP address is obtained as follows:

Phase	Description
1	In case on the LAN interface … • no IP address or subnet mask are configured (default value) AND the telindus24xx/lanInterface/mode attribute is set to routing, OR • no IP address or subnet mask are configured (default value) AND the telindus24xx/lanInterface/mode attribute is set to bridging (default value) AND no IP address or subnet mask are configured in the bridgeGroup (default value), … then the Telindus 2400 starts sending BootP requests every 10 seconds on its LAN interface. These requests contain the Telindus 2400 its MAC address.
2	The BootP server looks in its MAC address - IP address file. If the MAC address in the BootP request matches a MAC address in this file, the BootP server replies with the corresponding IP address and subnet mask. **Example** In the example above, the Telindus 2400 its MAC address is 00:C0:89:00:94:6F. The server replies with IP address 192.168.47.254 and corresponding subnet mask 255.255.255.0.
3	The Telindus 2400 uses this received IP address as its LAN IP address. It is stored in the Telindus 2400 its volatile memory. This means that after a cold boot, the Telindus 2400 has to request the LAN IP address again.

18.3 Obtaining the configuration with TFTP

Once the Telindus 2400 has obtained an IP address, it is reachable over its LAN interface. Now you can start a TMA or a Telnet session on the Telindus 2400 and configure it.

Alternatively the Telindus 2400 can retrieve its complete configuration without any user intervention. As long as the previously obtained IP addresses are not stored in non-volatile memory, the Telindus 2400 tries to get a complete configuration file from a TFTP server.

The configuration file and TFTP

The Trivial File Transfer Protocol is typically used in combination with BootP to obtain the configuration of a device from a TFTP server. The configuration file on this TFTP can be in a binary or an ASCII format. How to build such files is explained in 18.4 - Creating configuration files on page 673.

Getting the configuration file with TFTP

The Telindus 2400 asks for its configuration file as follows:

Phase	Description
1	The Telindus 2400 sends a DNS request on the interface for which it received an IP address. This request is a local broadcast message. If it sent over the WAN link, the peer router should have an IP helper address for the DNS server. If no reply is received within 10 seconds, this phase is repeated once more.
2	If a DNS reply is received, it contains the domain name. The Telindus 2400 only uses the hostname part of the domain name: *hostname.domain.toplevel_domain*.

<table>
<tr><th>Phase</th><th>Description</th></tr>
<tr><td>3</td><td>Now there are two possibilities:
<table>
<tr><th>If the host name is …</th><th>then …</th></tr>
<tr><td>known,</td><td>the router requests the file hostname.cms as a limited broadcast. hostname.cms is the router its configuration file in binary format.

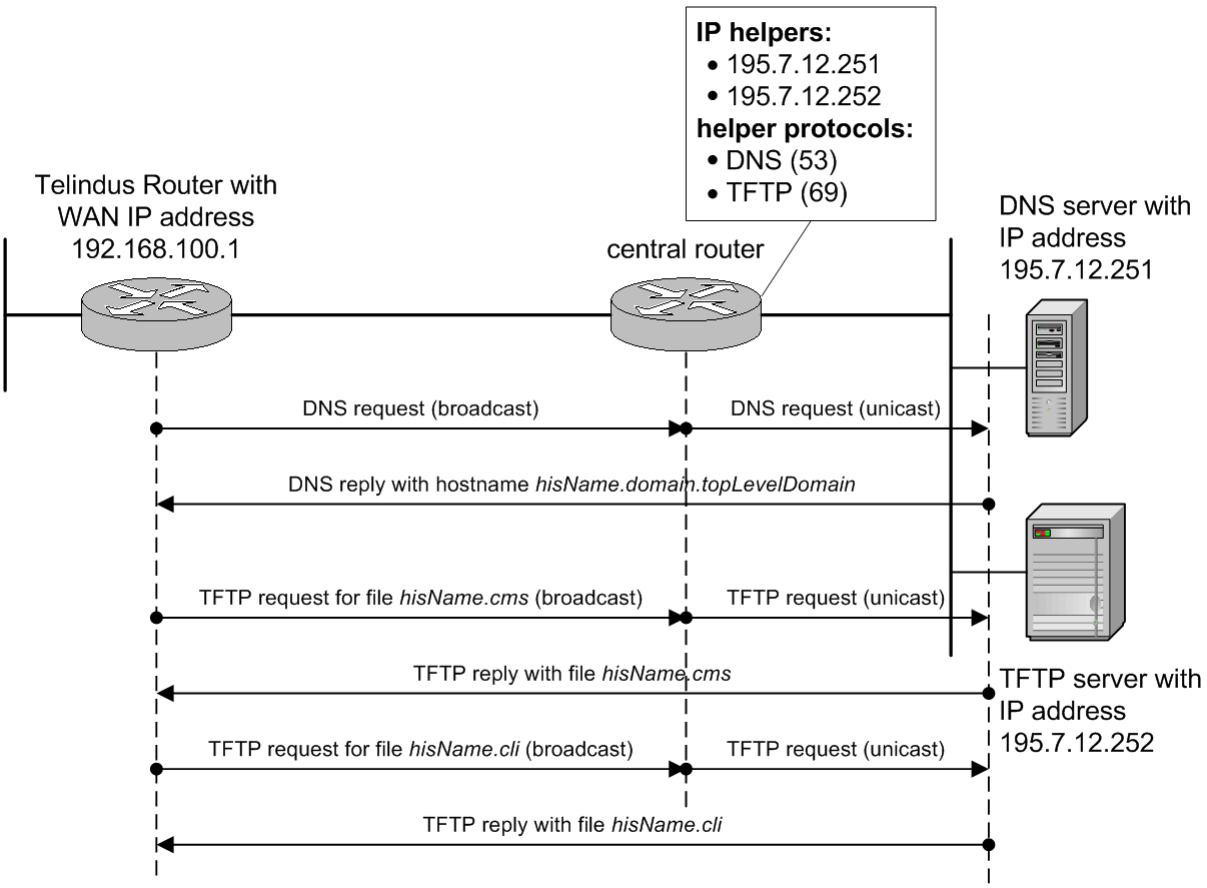
If this request is sent over the WAN link, the peer router should have an IP helper address for the TFTP server.

If no reply is received within 5 seconds, the router requests the file hostname.cli as a local broadcast. hostname.cli is the router its configuration file in ASCII format. Again there is a reply time-out of 5 seconds.

If still no valid answer is received, the router alternatively repeats both requests up to four times.</td></tr>
<tr><td>not known,</td><td>the procedure described above is executed with the file name hostname replaced by the concatenation of the decimal representation for each byte in the IP address, with leading zeroes and without dots in between the bytes.

Example, a router with IP address 192.168.100.1 requests the file 192168100001.cms or 192168100001.cli.</td></tr>
</table></td></tr>
<tr><td>4</td><td>If the Telindus 2400 received a valid configuration file, then it stores the configuration and possibly reboots. Else it restarts with phase 1.</td></tr>
</table>

The following figure illustrates the procedure as described in the table above. It shows the procedure over a WAN link. The IP address of the router is 192.168.100.1 and its hostname is *his_name*. In this example, the DNS server and TFTP server are on different machines. However, in reality these two services often reside on the same machine.



18.4 Creating configuration files

In 18.3 - Obtaining the configuration with TFTP on page 670, you have seen how you can get a configuration file with TFTP. The two possible configuration file formats used by TFTP are:

File type	Extension	How to create the configuration file
binary	.cms	Use the TMA export utility and choose the CMS file type. This is the most compact format. Refer to 18.5 - Creating a binary configuration file on page 674.
ASCII	.cli	Use the CLI user interface. Refer to 18.6 - Creating an ASCII configuration file on page 675. When you download an ASCII (*.cli) configuration file to the Telindus 2400, make sure that each line in this file contains no more than 500 characters.

18.5 Creating a binary configuration file

To create a configuration file in binary (*.cms) format, proceed as follows:

Step	Action
1	Start a TMA session on the Telindus 2400.
2	Make changes to its configuration (if necessary) in order to obtain the desired configuration. You do not have to send these configuration changes to the Telindus 2400.
3	Click on the *Export data to file* button: .
4	In the *Export configuration parameters* window, select the following: • Choose a directory where to save the file. • Enter a name for the file. • Make sure the file type is CMS. • Make sure the *Full configuration* option is selected.
5	Click on the *Save* button. The edited configuration of the Telindus 2400 is stored on the PC in binary format. The file contains the complete configuration including the *Activate Configuration* command. As a result, the configuration is immediately activated when downloaded with TFTP.

18.6 Creating an ASCII configuration file

To create a configuration file in ASCII format, you can use the CLI syntax as explained in the Maintenance tools manual (PDF). However, for the first time user it is easier to retrieve the configuration in the CLI format from the Telindus 2400.

There are two possible ways to create a configuration file in ASCII (*.cli) format:

- 18.6.1 - Creating an ASCII file using the TFTP get command on page 676
- 18.6.2 - Creating an ASCII file using the CLI get command on page 677

Do not use the TMA export utility for creating an ASCII type configuration file (not even when saving it as a TXT file). The resulting format is not compatible with the CLI format.

18.6.1 Creating an ASCII file using the TFTP *get* command

To create a configuration file in ASCII (*.cli) format using the TFTP *get* command, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 2400. For example by typing `tftp 10.0.11.1` at the command prompt of your UNIX station, where 10.0.11.1 is the LAN IP address of the Telindus 2400.
2	Get the configuration file of the Telindus 2400. **Example** `tftp> get CONFIG.CLI dest_file.cli` Where … • `get` is the TFTP command to retrieve a file, • `CONFIG.CLI` is the Telindus 2400 configuration file, • `dest_file.cli` is the destination file.
3	When the file transfer is finished, close the TFTP session.

18.6.2 Creating an ASCII file using the CLI *get* command

To create a configuration file in ASCII (*.cli) format using the CLI *get* command and Telnet logging, proceed as follows:

Step	Action
1	Start a Telnet session on the Telindus 2400. You are automatically in CLI mode.
2	Redirect the CLI output or log it to a file.
3	Make sure you are in the top object (telindus24xx) and in the "Edit Configuration" group.
4	Execute the `get -r` command.
5	Stop output redirection or logging.
6	In the redirected or logged file you now obtained, remove all input and output logging before the *get -r* command. Also remove the *get -r* command itself.
7	Now, modify the configuration file: **Step** / **Action** 1 – Change the string *GET*, now located at the beginning of the file, into *SET*. 2 – Type the string *Load Default Configuration* at the beginning of the file. 3 – Type the string *Activate Configuration* at the end of the file.
8	Save this file to a file with an extension **.cli*.

19 Downloading software

This chapter explains how to download loader software in the flash memory and application software to the file system of the Telindus 2400. It also shows how to download any other file to the file system of the Telindus 2400. But first it explains the difference between boot, loader and application software.

The following gives an overview of this chapter:

- 19.1 - What is boot, loader and application software? on page 680
- 19.2 - Downloading application software on page 682
- 19.3 - Downloading loader software on page 688
- 19.4 - Downloading files to the file system on page 690

19.1 What is boot, loader and application software?

What is boot software?

The boot software takes care of the initial phase in the start-up sequence of the Telindus 2400. It is located on the lowest software level. If the Telindus 2400 only loads its boot software, then we say that the Telindus 2400 runs in *boot mode*.

The Telindus 2400 …

- runs in boot mode if only the boot software is present, but no loader or application software is present.
- can temporarily be forced to run in boot mode by using the -b option of the TML command when running in loader mode. Refer to 19.2.3 - Downloading application software using TML on page 685.

In boot mode …

- you can download loader software (using TML).
- you cannot download application software.
- you cannot establish a TMA session. You can only use TML to download loader software.

Boot software is a fixed software. This means you cannot download new boot software.

What is loader software?

The loader software takes care of the second phase in the start-up sequence of the Telindus 2400. It is located on the middle software level. If the Telindus 2400 loads its boot and loader software, then we say that the Telindus 2400 runs in *loader mode*.

The Telindus 2400 …

- runs in loader mode if the boot and loader software is present, but no application software is present.
- can be forced to run in loader mode by using a DIP switch. This may be necessary in case a software download failed or a flash memory error occurred making the Telindus 2400 inaccessible or even inoperative. Refer to 19.2.5 - Downloading application software in loader mode on page 687.

In loader mode …

- you can download loader software provided you use the -b option of the TML command, temporarily forcing the Telindus 2400 to run in boot mode. Refer to 19.2.3 - Downloading application software using TML on page 685.
- you can download application software (using TML).
- you cannot establish a TMA session. You can only use TML to download loader and application software.

What is application software

The application software, also called control software or firmware, completely controls the Telindus 2400. It is located on the highest software level. If the Telindus 2400 loads its boot, loader and application software, then we say that the Telindus 2400 runs in *application mode*.

The Telindus 2400 can store two complete application software versions. It stores these on the file system under the names CONTROL1 and CONTROL2:

- You can check which application software version is stored in CONTROL 1 and 2 by checking the status attributes telindus24xx/flash1Version on page 482 and telindus24xx/flash2Version on page 482.
- You can check which application software version is currently being used (CONTROL1 or 2) by checking the status attribute telindus24xx/activeFlash on page 483.
- You can determine which of the 2 application software versions the Telindus 2400 uses after a cold boot (CONTROL1 or 2) by setting the configuration attribute telindus24xx/bootFromFlash on page 307.

In application mode …

- you can download application software (using TMA, TFTP or TML).
- you can establish a TMA session.

19.2 Downloading application software

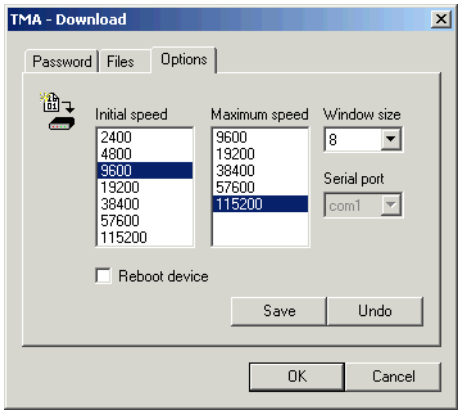
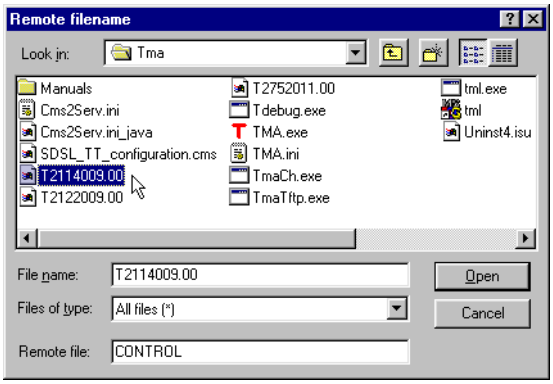
This section shows how you can download new application software into the Telindus 2400 and this using different tools.

The following gives an overview of this section:

- 19.2.1 - Downloading application software using TMA on page 683
- 19.2.2 - Downloading application software using TFTP on page 684
- 19.2.3 - Downloading application software using TML on page 685
- 19.2.4 - Downloading application software using FTP on page 686
- 19.2.5 - Downloading application software in loader mode on page 687

19.2.1 Downloading application software using TMA

To download application software to the Telindus 2400 using TMA, proceed as follows:

Step	Action
1	Establish a link between TMA and the Telindus 2400 either over a serial or an IP connection. Refer to 4 - Maintaining the Telindus 2400 on page 41.
2	In the TMA window select *Tools* → *Download…*
3	In case you made … • an IP connection, skip this step. • a serial connection, select the *Options* tab in the *TMA - Download* window. Then set the following: - Set the initial transfer speed to 9600 bps. - Select a maximum transfer speed. If you select e.g. 115200 bps, then the actual transfer speed will be negotiated between 9600 bps and 115200 bps. 
4	In the *TMA - Download* window, select the *Configuration* tab and click on *Add…*
5	In the *Remote filename* window, do the following: 1. Select the file you want to download (e.g. T1234001.00). 2. Type `CONTROL` in the *Remote file* field. 3. Click on *Open*. 
6	If you are currently connected to the Telindus 2400 without write access, then you can enter a password in the *Password* tab which gives you write access. Else leave the *Password* tab blank.
7	When the *TMA - Download* window reappears, click on *OK*. ⇒A window opens and shows the download progress.

19.2.2 Downloading application software using TFTP

When downloading with TMA over an IP connection, you actually evoke TFTP (Trivial File Transfer Protocol) through TMA. You can also use TFTP without opening TMA.

To download application software to the Telindus 2400 using TFTP, proceed as follows:

Step	Action
1	Start a TFTP session on the Telindus 2400. For example by typing `tftp 10.0.11.1` at the command prompt of your computer, where 10.0.11.1 is the LAN IP address of the Telindus 2400. If a write access password is configured on the Telindus 2400, you can either enter it now or when you actually download the application software (see step 3).
2	Set the following TFTP parameters: • Set the retransmission time-out to at least 20 seconds. The syntax to do this is typically `rexmt 20`. • Set the total TFTP time-out sufficiently large (e.g. 40 seconds). The syntax to do this is typically `timeout 40`. • Set the transfer mode to binary (octet) format. The syntax to do this is typically `binary` or `octet`.
3	Type the following command: `tftp> put Txxxxxxx.00 CONTROL?my_pwd` Where … • `put` is the TFTP command to send a file. • `Txxxxxxx.00` is the application software file (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is an application software file. • `?my_pwd` is the write access password as configured in the Telindus 2400. If no password has been configured or if you already entered one when starting the TFTP session (see step 1), you may omit the ? and the password.
4	When the file transfer is finished, close the TFTP session.

19.2.3 Downloading application software using TML

When downloading with TMA over a serial connection, you actually evoke TML (Telindus Memory Loader) through TMA. You can also use TML without opening TMA.

To download application software to the Telindus 2400 using TML, proceed as follows:

Step	Action
1	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 2400.
2	Open a DOS window on your computer.
3	Go to the directory where the TML executable is located. Typically this is *C:\Program Files\TMA*.
4	Place the application software file you want to download in this directory.
5	Type the following command to download: `tml -c1 -v -fTxxxxxxx.00@CONTROL?my_pwd` where … • `tml` is the executable (Telindus Memory Loader) to download files to the Telindus devices through their control port. • `-c1` specifies the COM port of the computer connected to the Telindus 2400 (in this example COM1). • `-v` returns graphical information on the download status. • `-fTxxxxxxx.00` is the software file you want to download (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is an application software file. • `?my_pwd` is the write access password as configured in the Telindus 2400. If no password has been configured, you may omit the ? and the password. To see a list of all the possible TML options: type `TML` in your DOS windows and press the ENTER key.
6	If you press the ENTER key, the software download begins. If you used the *-v* option together with the TML command, a graphical bar shows the download progress.

19.2.4 Downloading application software using FTP

To download application software to the Telindus 2400 using FTP, proceed as follows:

Step	Action
1	Start an FTP session on the Telindus 2400. For example by typing `ftp 10.0.11.1` at the command prompt of your computer, where 10.0.11.1 is the LAN IP address of the Telindus 2400. If a write access password is configured on the Telindus 2400, you can either enter it now or when you actually download the application software (see step 3).
2	Make sure the transfer mode is set to binary (octet) format. The syntax to do this is typically `binary`.
3	Type the following command: `ftp> put Txxxxxxx.00 CONTROL?my_pwd` Where … • `put` is the FTP command to send a file. • `Txxxxxxx.00` is the application software file (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is an application software file. • `?my_pwd` is the write access password as configured in the Telindus 2400. If no password has been configured or if you already entered one when starting the FTP session (see step 1), you may omit the ? and the password.
4	When the file transfer is finished, close the FTP session.

19.2.5 Downloading application software in loader mode

When a software download failed or when a flash memory error occurs, it may be possible that the Telindus 2400 becomes inaccessible or even inoperative. In that case, new application software can still be downloaded by forcing the Telindus 2400 in loader mode and using TML to download new application software. Do this by means of the *loader mode* DIP switch.

To download application software to a Telindus 2400 in loader mode, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 40.
2	Set DIP switch bank DS1 position 1 to *off*. Refer to 3.1 - The Telindus 2400 motherboard on page 38 to locate this DIP switch bank.
3	Slide the bottom in the cover again without fastening the screws and reconnect the power supply. ⇒The Telindus 2400 reboots in loader mode.
4	Now proceed as explained in 19.2.3 - Downloading application software using TML on page 685.
5	When the software download is finished, again disconnect the power supply and open the housing.
6	Reset DIP switch bank DS1 position 1 to *on*.
7	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 40 and reconnect the power supply.

19.3 Downloading loader software

When you want to download new loader software, the Telindus 2400 first has to be running in loader mode and then it has to be forced to run in boot mode using the -b option of the TML command while downloading new loader software.

To download loader software to the Telindus 2400, proceed as follows:

Step	Action
1	Disconnect the power supply and open the housing as described in 3.3 - Opening and closing the housing on page 40.
2	Set DIP switch bank DS1 position 1 to *off*. Refer to 3.1 - The Telindus 2400 motherboard on page 38 to locate this DIP switch bank.
3	Slide the bottom in the cover again without fastening the screws and reconnect the power supply. ⇒The Telindus 2400 reboots in loader mode.
4	Connect a serial port of your computer (e.g. COM1) through a straight DB9 male - female cable with the control connector of the Telindus 2400.
5	Open a DOS window on your computer.
6	Go to the directory where the TML executable is located. Typically this is *C:\Program Files\TMA*.
7	Place the software file you want to download in this directory.
8	Type the following command: `tml -c1 -v -b -fTxxxxxxx.00@CONTROL?my_pwd` where … • `tml` is the executable (Telindus Memory Loader) to download files to the Telindus devices through their control port. • `-c1` specifies the COM port of the computer connected to the Telindus 2400 (in this example COM1). • `-v` returns graphical information on the download status. • `-b` puts the Telindus 2400 in boot mode. This is only necessary when you want to download loader software. • `-fTxxxxxxx.00` is the software file you want to download (e.g. T1234001.00). • `CONTROL` (in capitals!) specifies that the file being downloaded is a loader software file. • `?my_pwd` is the write access password as configured in the Telindus 2400. If no password has been configured, you may omit the ? and the password. To see a list of all the possible TML options: type `TML` in your DOS windows and press the ENTER key.

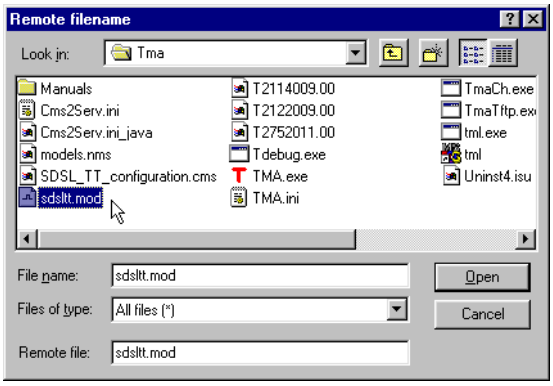
Step	Action
9	If you press the ENTER key, the software download begins. If you used the *-v* option together with the TML command, a graphical bar shows the download progress.
10	When the software download is finished, again disconnect the power supply and open the housing.
11	Reset DIP switch bank DS1 position 1 to *on*.
12	Properly replace the cover as described in 3.3 - Opening and closing the housing on page 40 and reconnect the power supply.

19.4 Downloading files to the file system

You might want to download other files than the firmware files only. In fact, any file can be downloaded to the file system of the Telindus 2400. You can do this using the same tools you use to download application software. These tools are:

- TMA (refer to 19.2.1 - Downloading application software using TMA on page 683).
- TFTP (refer to 19.2.2 - Downloading application software using TFTP on page 684).
- TML (refer to 19.2.3 - Downloading application software using TML on page 685).
- TFTP (refer to 19.2.4 - Downloading application software using FTP on page 686).

The major difference is that instead of specifying `CONTROL` as target filename for the application software, you now can specify any filename as target filename.

Tool	Example
TMA	In the *Remote filename* window, do the following: 1. Select the file you want to download (e.g. *sdsltt.mod*). 2. Type the target filename in the *Remote file* field (e.g. *sdsltt.mod*). 3. Click on *Open*. 
(T)FTP and TML	• `tftp> put filename1.ext filename2.ext?my_pwd` • `ftp> put filename1.ext filename2.ext?my_pwd` • `tml -c1 -v -ffilename1.ext@filename2.ext?my_pwd` Where … • `filename1.ext` is the source filename. This is a file on your computer. • `filename2.ext` is the target filename. This is the filename the source file will get when it is placed on the file system. Source and target filename may be the same, but if wanted, you may specify a different target filename. Example: • `tftp> put models.nms models.nms?pwd123` • `tml -c1 -v -fmodels.nms@models.nms?pwd123`

20 Technical specifications

This chapter gives the technical specifications of the Telindus 2400. The following gives an overview of this chapter:

- 20.1 - Telindus 2400 models on page 692
- 20.2 - Power requirements on page 693
- 20.3 - Control connector specifications on page 694
- 20.4 - Station clock connector specifications on page 695
- 20.5 - Alarm in connector specifications on page 696
- 20.6 - Alarm out connector specifications on page 697
- 20.7 - xDSL line specifications on page 698
- 20.8 - LAN interface specifications on page 703
- 20.9 - TIM interface specifications on page 704
- 20.10 - ATM encapsulation specifications on page 707
- 20.11 - PPP encapsulation specifications on page 707
- 20.13 - IP routing specifications on page 709
- 20.14 - Bridging specifications on page 709
- 20.15 - Routing and bridging performance specifications on page 709
- 20.16 - ATM switching performance specifications on page 709
- 20.17 - Maintenance and management support on page 710
- 20.18 - Memory specifications on page 710
- 20.19 - Dimensions on page 710
- 20.20 - Safety compliance on page 711
- 20.21 - Over-voltage and over-current protection compliance on page 711
- 20.22 - EMC compliance on page 711
- 20.23 - Environmental compliance on page 711

20.1 Telindus 2400 models

The Telindus 2400 series consists of the following models and sub-models:

		Number of lines		
		8	16	24
ADSL lines	Annex A (ATM only)	**Telindus 2401** Sub-models: • -48 Vdc, with POTS splitter • -48 Vdc, without POTS splitter • -48 Vdc/Vac, with POTS splitter • -48 Vdc/Vac, without POTS splitter	**Telindus 2402** -48 Vdc and without POTS splitter only.	**Telindus 2403** -48 Vdc and without POTS splitter only.
	Annex B (ATM only)	**Telindus 2401** Sub-models: • -48 Vdc, with POTS splitter • -48 Vdc, without POTS splitter • -48 Vdc/Vac, with POTS splitter • -48 Vdc/Vac, without POTS splitter	**Telindus 2402** -48 Vdc and without POTS splitter only.	**Telindus 2403** -48 Vdc and without POTS splitter only.
SHDSL lines	ATM	**Telindus 2421** Sub-models: • -48 Vdc • -48 Vdc/Vac	**Telindus 2422** -48 Vdc only	**Telindus 2423** -48 Vdc only

20.2 Power requirements

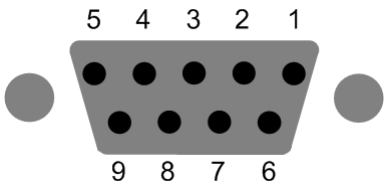
- Connectors:
  - Standard IEC power socket[1] for the 230 Vac power input
  - 1 or 2 mini-combicon power sockets[2] for the -48 Vdc power input (also 1 or 2 mini-combicon power plugs are delivered with the Telindus 2400)
- Maximum wire cross-section that can be inserted in the mini-combicon power plug: 1.5 mm^2
- Power redundancy:
  - Vdc/Vac models: possibility to connect one 230 Vac power supply and one -48 Vdc power supply
  - Vdc models: possibility to connect two -48 Vdc power supplies
- Power consumption: 15 W

1. The standard IEC power socket is only present in case of a Vdc/Vac model.
2. 1 mini-combicon power socket in case of a Vdc/Vac model. 2 mini-combicon power sockets in case of a Vdc model.

20.3 Control connector specifications

- Connector: female DB9 labelled CTRL
- Applicable standards: ITU-T V.24, V.28, EIA/TIA 574
- Data:
  - asynchronous
  - 9600 bps
  - 8 data bits
  - no parity
  - 1 stop bit
  - no flow control

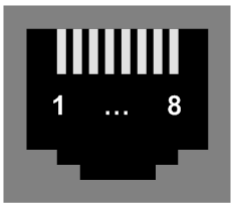
The control connector has the following pin layout:

Pin	Signal		DCE	Figure
1	not used	-	-	
2	Receive Data	RxD	output	
3	Transmit Data	TxD	input	
4	not used	-	-	
5	GND	GND	-	
6	not used	-	-	
7	not used	-	-	
8	not used	-	-	
9	not used	-	-	

20.4 Station clock connector specifications

- Connector: RJ45
- Impedance: 120 ohm balanced
- Physical and electrical compliance: ITU-T G.703
- Cable to be used: 4*2*CAT5E shielded twisted pair
- Input signal frequency: 2048 Khz

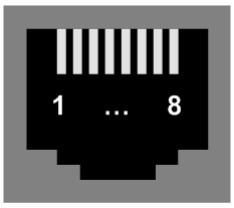
The following table shows the connector layout of the station clock connector:

Pin	Signal	DCE	Figure
1	in A	input	
2	in B	input	
3	shielding ground	-	
4	out A	output	
5	out B	output	
6	shielding ground	-	
7	not connected	-	
8	not connected	-	

20.5 Alarm in connector specifications

- Connector: RJ45

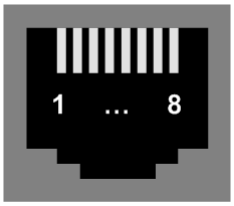
The following table shows the connector layout of the alarm in connector:

Pin	Signal	Figure
1	alarm contact 1	
2	alarm contact 2	
3	alarm contact 3	
4	alarm contact 4	
5	alarm contact 5	
6	alarm contact 6	
7	alarm contact 7	
8	common return path	

20.6 Alarm out connector specifications

- Connector: RJ45
- Alarm contact in open condition: maximum 60 Vdc or 40 Vac
- Alarm contact in closed condition: maximum 1 A resistive load
- Total switching power: 62.5 VA or 60 W

The following table shows the connector layout of the alarm in connector:

Pin	Signal	Figure
1	low alarm contact - closed	
2	low alarm contact - common	
3	low alarm contact - open	
4	high alarm contact - closed	
5	high alarm contact - common	
6	high alarm contact - open	
7	not connected	
8	not connected	

20.7 xDSL line specifications

This section gives the xDSL line specifications of the Telindus 2400. The following gives an overview of this section:

- 20.7.1 - SHDSL line specifications on page 699
- 20.7.2 - ADSL line specifications on page 700
- 20.7.3 - xDSL line connector specifications on page 701
- 20.7.4 - ADSL line connector specifications with POTS splitter on page 702

20.7.1 SHDSL line specifications

- SHDSL line access:
  - Telindus 2421: 8 x single pair, possibility to create dual pairs through configuration
  - Telindus 2422: 16 x single pair, possibility to create dual pairs through configuration
  - Telindus 2423: 24 x single pair, possibility to create dual pairs through configuration
- Connector: 50 pins TELCO[1]
- Impedance: 135 ohm
- Cable to be used: 25*2*CAT5 twisted pair (Also twisted *inside* the connector assembly!)
- Coding: TC PAM, compliant to ITU-T G.991.2 (G.SHDSL) and ETSI TS 101524
- Line speeds:
  - Single pair: N x 64 kbps (N = 3 … 36)
  - Dual pair: N x 128 kbps (N = 3 … 36)
- Handshaking: compliant G.994.1 (automatic speed negotiation) or fixed speed
- Performance monitoring: compliant G.826 (errored seconds, severely errored seconds, unavailability seconds)
- Encapsulation: ATM

Maximum covered distance

The following table gives the maximum covered distance over a noise-free line:

		Covered distance (km)					
Line speed (kbps)		**Wire diameter (mm)**					
1 Pair	**2 Pair**	**0.4**	**0.5**	**0.6**	**0.8**	**1.0**	**1.2**
64	128	11,0	15,1	21,5	27,2	38,2	42,4
128	256	8,0	11,0	15,6	19,8	27,8	30,8
256	512	8,2	11,3	16,0	20,3	28,5	31,6
512	1024	7,2	9,9	14,0	17,8	25,0	27,7
1024	2048	5,5	7,6	10,7	13,6	19,1	21,2
1536	3072	4,0	5,5	7,8	9,9	13,9	15,4
2048	4096	4,2	5,8	8,2	10,4	14,6	16,2
2304	4608	4,0	5,5	7,8	9,9	13,9	15,4

These values are valid for all hardware and firmware revisions. Also note that these values are only valid when using the correct, properly twisted cable.

1. Depending on the Telindus 2400 model 8, 16 or 24 line pairs are wired.

20.7.2 ADSL line specifications

- ADSL line access:
  - Telindus 2401: 8 x single pair
  - Telindus 2402: 16 x single pair
  - Telindus 2403: 24 x single pair
- Connector: 50 pins TELCO[1]
- Impedance: 135 ohm
- Cable to be used: 25*2*CAT5 twisted pair (Also twisted *inside* the connector assembly!)
- Coding: compliant to ITU-T G.992.1 (ADSL G.dmt), ITU-T G.992.2 (ADSL G.Lite), ETSI TS 101 388 v1.3.1
- Support for ITU-T Annex A (POTS) or Annex B (POTS and ISDN)
- Internal/external POTS or ISDN splitter:
  - Telindus 2401: available with or without internal splitter
  - Telindus 2402 and 2403: no internal splitter, external splitter available
- Line speeds:
  - Downstream: 32 kbps up to 10592 kbps
  - Upstream: 32 kbps up to 1024 kbps
- Performance monitoring: compliant G.826 (errored seconds, severely errored seconds, unavailability seconds)
- Encapsulation: ATM

1. Depending on the Telindus 2400 model 8, 16 or 24 line pairs are wired.

20.7.3 xDSL line connector specifications

Depending on the Telindus 2400 version, 8, 16 or 24 pin pairs are wired.

The following figure shows the 50 pins TELCO line connector:

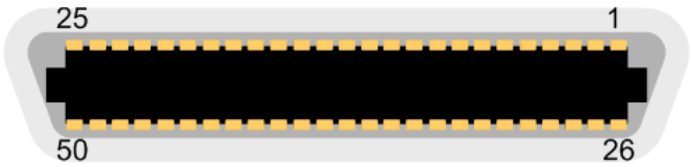
The following table shows the connector layout of the 50 pins TELCO line connector:

Pin	Signal	Pin	Signal
1	line pair 1 - ring	26	line pair 1 - tip
2	line pair 2 - ring	27	line pair 2 - tip
3	line pair 3 - ring	28	line pair 3 - tip
4	line pair 4 - ring	29	line pair 4 - tip
5	line pair 5 - ring	30	line pair 5 - tip
6	line pair 6 - ring	31	line pair 6 - tip
7	line pair 7 - ring	32	line pair 7 - tip
8	line pair 8 - ring	33	line pair 8 - tip
9	line pair 9 - ring	34	line pair 9 - tip
10	line pair 10 - ring	35	line pair 10 - tip
11	line pair 11 - ring	36	line pair 11 - tip
12	line pair 12 - ring	37	line pair 12 - tip
13	line pair 13 - ring	38	line pair 13 - tip
14	line pair 14 - ring	39	line pair 14 - tip
15	line pair 15 - ring	40	line pair 15 - tip
16	line pair 16 - ring	41	line pair 16 - tip
17	line pair 17 - ring	42	line pair 17 - tip
18	line pair 18 - ring	43	line pair 18 - tip
19	line pair 19 - ring	44	line pair 19 - tip
20	line pair 20 - ring	45	line pair 20 - tip
21	line pair 21 - ring	46	line pair 21 - tip
22	line pair 22 - ring	47	line pair 22 - tip
23	line pair 23 - ring	48	line pair 23 - tip
24	line pair 24 - ring	49	line pair 24 - tip
25	shield	50	shield

20.7.4 ADSL line connector specifications with POTS splitter

This applies on Telindus 24x1 models with internal POTS splitter only.

The following figure shows the 50 pins TELCO line connector:



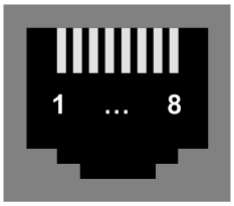
The following table shows the connector layout of the 50 pins TELCO line connector:

Pin	Signal	Pin	Signal
1	ADSL + POTS line pair 1 - ring	26	ADSL + POTS line pair 1 - tip
2	ADSL + POTS line pair 2 - ring	27	ADSL + POTS line pair 2 - tip
3	ADSL + POTS line pair 3 - ring	28	ADSL + POTS line pair 3 - tip
4	ADSL + POTS line pair 4 - ring	29	ADSL + POTS line pair 4 - tip
5	ADSL + POTS line pair 5 - ring	30	ADSL + POTS line pair 5 - tip
6	ADSL + POTS line pair 6 - ring	31	ADSL + POTS line pair 6 - tip
7	ADSL + POTS line pair 7 - ring	32	ADSL + POTS line pair 7 - tip
8	ADSL + POTS line pair 8 - ring	33	ADSL + POTS line pair 8 - tip
9	not connected	34	not connected
10	not connected	35	not connected
11	not connected	36	not connected
12	not connected	37	not connected
13	not connected	38	not connected
14	not connected	39	not connected
15	not connected	40	not connected
16	not connected	41	not connected
17	POTS line pair 1 - ring	42	POTS line pair 1 - tip
18	POTS line pair 2 - ring	43	POTS line pair 2 - tip
19	POTS line pair 3 - ring	44	POTS line pair 3 - tip
20	POTS line pair 4 - ring	45	POTS line pair 4 - tip
21	POTS line pair 5 - ring	46	POTS line pair 5 - tip
22	POTS line pair 6 - ring	47	POTS line pair 6 - tip
23	POTS line pair 7 - ring	48	POTS line pair 7 - tip
24	POTS line pair 8 - ring	49	POTS line pair 8 - tip
25	shield	50	shield

20.8 LAN interface specifications

- Connector: RJ45 (EIA/TIA 568B)
- Cable to be used:
  - 4*2*CAT5E unshielded twisted pair
  - straight-through cable or crossover cable
- Applicable standards: IEEE 802.3 (10Mbps Ethernet), IEEE 802.3u (100Mbps Ethernet)
- Speed: 10/100 Mbps / half/full duplex, fixed or auto-sense (configurable)
- Wiring: auto crossover

The following table shows the connector layout of the RJ45 LAN interface connector:

Pin	Signal	I/O	Figure
1	transmit (positive)	output	
2	transmit (negative)	output	
3	receive (positive)	input	
4	not used	-	
5	not used	-	
6	receive (negative)	input	
7	not used	-	
8	not used	-	

The LAN interface supports auto crossover. Therefore, you can use both straight-through and crossover cables. The transmit / receive swapping happens automatically when necessary.

20.9 TIM interface specifications

This section gives the specifications of the Telindus Interface Modules (TIMs) that can be used in the Telindus 2400. The following gives an overview of this section:

- 20.9.1 - 4 port Ethernet TIM interface specifications on page 705
- 20.9.2 - 6E1 TIM interface specifications on page 705
- 20.9.3 - E3/T3 TIM interface specifications on page 706

20.9.1 4 port Ethernet TIM interface specifications

- Telindus Interface Module, can be inserted in the interface slot of the Telindus 2400
- Connector: 4 x RJ45 (EIA/TIA 568B)
- Cable to be used: 4*2*CAT5E unshielded twisted pair
- Encapsulation: IEEE 802.3 (10Mbps Ethernet), IEEE 802.3u (100Mbps Ethernet)
- Speed: 10/100 Mbps / half/full duplex, auto-sense (not fixed configurable)
- Wiring: auto crossover

For more information on the hardware of this interface (e.g. connector layout, etc.), refer to the installation guide of the 4 port Ethernet interface (PDF).

20.9.2 6E1 TIM interface specifications

- Telindus Interface Module, can be inserted in the interface slot of the Telindus 2400
- Connector: 6 x RJ45 (DTE)
- Impedance: 120 ohm balanced
- Physical and electrical compliance: ITU-T G.703
- Cable to be used: 4*2*CAT5E shielded twisted pair
- Coding: AMI or HDB3 (configurable)
- Speed: 2 Mbps per E1 interface
- Clocking: external, internal (configurable)
- Framing: framed, framing compliant to ITU-T G.704
- Time slots: N x 64 kbps, with N = 31
- CRC4 insertion: enabled, disabled or automatic detection (configurable), frame alignment and cyclic redundancy check compliant to ITU-T G.706
- Defect detection: compliant to ITU-T G.775
- Performance monitoring: compliant to ITU-T G.821 and G.826
- Jitter and wander: compliant to G.823
- Encapsulation: ATM IMA
- ATM config:
  - idle cell format: ITU (fixed)
  - scrambling: enabled, disabled (configurable)
  - coset: enabled, disabled (configurable)

For more information on the hardware of this interface (e.g. connector layout, etc.), refer to the installation guide of the 6E1 interface (PDF).

20.9.3 E3/T3 TIM interface specifications

- Telindus Interface Module, can be inserted in the interface slot of the Telindus 2400
- E3/T3 TIM interface types:
  - Single E3/T3 TIM: one E3/T3 interface
  - Dual E3/T3 TIM: two independent E3/T3 interfaces
- Connector: 2 x BNC (DTE) per E3/T3 interface
- Impedance: 75 ohm balanced
- Physical and electrical compliance: ITU-T G.703
- Cable to be used: coaxial cable
- Mode: E3
- Speed:
  - E3 mode: 34.368 Mbps
- Clocking: external, internal (configurable)
- Defect detection: compliant to ITU-T G.775
- Performance monitoring: compliant to ITU-T G.821 and G.826
- Jitter and wander: compliant to G.823
- Encapsulation: ATM
- ATM config:
  - idle cell format: ITU (fixed)
  - scrambling: enabled (fixed)

For more information on the hardware of this interface (e.g. connector layout, etc.), refer to the installation guide of the E3/T3 interface (PDF).

20.10 ATM encapsulation specifications

- ATM cell format ITU-T I.311, I.321, I.361, I.432
- ATM forum UNI 3.1/4.0 PVCs
- ATM forum ILMI 3.1/4.0
- OAM F4/F5 loopback support (ITU-T I.610)
- ATM Forum Traffic Management 4.0 service type UBR
- Inverse ARP for automatic gateway configuration
- Support of up to 32 ATM PVCs
- ATM VPI range: 0 - 15
- ATM VCI range:
  - on xDSL interface of Telindus 24x1: 32 - 512
  - on xDSL interface of Telindus 24x2 and 24x3: 32 - 256
  - on TIM 6E1 (in IMA bundle): 32 … 512
  - on TIM E3/T3: 32 … 512
- Supported higher layer protocols
  - Classical IP (RFC 1577)
  - Ethernet (RFC 2684)
  - PPPoA (RFC 2364)
  - PPPoE (RFC 2516)
- Multi-protocol encapsulation
  - LLC
  - VC

20.11 PPP encapsulation specifications

- Encapsulation compliant with RFC 1661, RFC 1662
- LCP
- IPCP (RFC 1332)
- BCP (RFC 2878)
- CCP (RFC 1962) with Predictor compression algorithm (RFC 1978)
- CHAP authentication with MD5 hashing (RFC 1994), unidirectional or bi-directional authentication
- PAP authentication (RFC 1334), unidirectional or bi-directional authentication
- MLPPP (RFC 1990)

20.12 IP routing specifications

- IP (RFC 791)
- ARP (RFC 826)
- Static routing, RIP1 (RFC 1058), RIP2 with MD5 hashing and authentication (RFC 2453)
- Router requirements (RFC 1812)
- Standard and extended access filtering
- NAT (Network Address Translation) with dynamic or static IP address conversion
- PAT (Port Address Translation) (RFC 3022)
- BOOTP/DHCP server, relay agent (RFC 2131, RFC 2132)
- BOOTP client (RFC 951)
- Numbered/unnumbered WAN interface
- DiffServ priority tagging and queuing (RFC 2474, RFC 2475)
- L2TP tunnelling (RFC 2661)
- IPSEC security (RFC 2401 up to RFC 2411)

20.13 Bridging specifications

- Bridging with spanning tree protocol (IEEE 802.1D)
- VLAN interconnect and tagging (IEEE 802.1Q)
- VLAN priority queuing (IEEE 802.1P)
- Integrated Routing and Bridging (IRB)

20.14 Routing and bridging performance specifications

- Full forwarding performance of 300,000 packets per second

20.15 ATM switching performance specifications

- Full forwarding performance of 800,000 packets per second

20.16 Maintenance and management support

- Local console (Command Line Interface or ATWIN)
- TELNET (Command Line Interface or ATWIN) (RFC 854)
- TMA (Telindus Maintenance Application)
- HTTP web interface (RFC 2616)
- TFTP configuration download (RFC 1350)
- PING (RFC 792)
- SNMP MIB2 (RFC 1213), private MIB
- Software flash download
- TMA CLI[1]
- TMA Element Management[1]
- TMA for HP OpenView[1]
- 2 alarm output contacts
- 7 customisable alarm input contacts

20.17 Memory specifications

- Flash memory: 16 Mb
- RAM: 32 Mb

20.18 Dimensions

- Height: 44.45 mm (one 19” rack unit)
- Width: 440 mm (without rack mount brackets)
- Depth: 225 mm
- Weight: 3.6 kg

1. Not included.

20.19 Safety compliance

- EN60950
- Class 1 equipment for Table Tops with 115/230 Vac internal power supply.
- Class 3 equipment for …
  - Table Tops with 115/230 Vac external power supply adapter
  - Table Tops with -48 Vdc internal power supply
  - Card Versions.

20.20 Over-voltage and over-current protection compliance

The over-voltage and over-current protection complies with ITU-T K.44 and ETSI ETS 300 386-2 recommendations.

20.21 EMC compliance

- EN55022 B Emissions
- EN55024 Immunity
- EN61000-3-2 Harmonics
- EN61000-3-3 Voltage fluctuations and flicker
- EN61000-4-2 ESD
- EN61000-4-3 Radiated immunity
- EN61000-4-4 EFT/burst
- EN61000-4-5 Surge
- EN61000-4-6 Conducted immunity
- EN61000-4-8 Power magnetic field immunity
- EN61000-4-11 Voltage dips & drops
- ENV50204 Radiated immunity against digital radio telephone

20.22 Environmental compliance

- Storage conditions: ETSI ETS 300 019-1-1 Class 1.1. In addition, the storage temperature has to be between -25 to +70°C
- Transport conditions : ETSI ETS 300 019-1-2 Class 2.3
- Stationary use conditions: ETSI ETS 300 019-1-3 Class 3.2. In addition, the requirements below apply:
  - relative humidity 5 to 95% non-condensing and ambient operational temperature -5 to 45°C
    or
  - relative humidity 0 to 95% non-condensing and ambient operational temperature -10 to 50°C
- Maximum altitude: 3000m
- International protection (IP) class of protection against solid and liquids: IP40

Annex

Annex A: common TCP and UDP numbers

The following table shows the port numbers for a number of common protocols using TCP and UDP as transport protocol. As far as possible, the same port numbers are used for TCP as for UDP. A complete list can be found in the RFCs (Requests For Comment).

Port No	Protocol	UDP/TCP	Description
20	ftp-data	TCP	File Transfer (Default Data)
21	ftp	TCP	File Transfer (Control)
23	telnet	TCP	Telnet
25	smtp	TCP	Simple Mail Transfer Protocol
37	time	UDP/TCP	Time Server
42	nameserver	UDP	Host Name Server
53	domain	UDP/TCP	Domain Name Server
65	tacacs-ds	UDP/TCP	TACACS-Database Service
67	bootps	UDP	Bootstrap Protocol Server
68	bootpc	UDP	Bootstrap Protocol Client
69	tftp	UDP	Trivial File Transfer
80	www-http	TCP	World Wide Web HTTP
119	nntp	TCP	Network News Transfer Protocol
137	netbios-ns	UDP	NETBIOS Name Service
138	netbios-dgm	UDP	NETBIOS Datagram Service
139	netbios-ssn	UDP	NETBIOS Session Service
161	snmp	UDP	SNMP
162	snmptrap	UDP	SNMPTRAP
1728	telindus	UDP	Telindus Protocol used by TMA

Annex B: product information

The following table displays the product information of the Telindus 2400:

Sales code	Product name	Description
182736	TELINDUS 2401 ADSL ANNEX A BU 48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Without internal line splitter option. Redundant 48Vdc. Manufactured on order +3 month.
182737	TELINDUS 2401 ADSL ANNEX A BU AC/ 48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Without internal line splitter option. 48Vdc and AC power. Manufactured on order +3 month.
182573	TELINDUS 2401 ADSL ANNEX A S_CTRY1 BU 48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for BEL, NL, IT, Hungary, CHE & FR) . Redundant 48Vdc. Manufactured on order +3 month.
182735	TELINDUS 2401 ADSL ANNEX A S_CTRY1 BU AC/48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for BEL, NL, IT, Hungary, CHE & FR) . 48Vdc and AC power. Manufactured on order +3 month.
185635	TELINDUS 2401 ADSL ANNEX A S_CTRY2 BU 48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for Poland) . Redundant 48Vdc. Manufactured on order +3 month.
185638	TELINDUS 2401 ADSL ANNEX A S_CTRY2 BU AC/48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for Poland) . 48Vdc and AC power. Manufactured on order +3 month.
185636	TELINDUS 2401 ADSL ANNEX A S_CTRY3 BU 48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for UK) . Redundant 48Vdc. Manufactured on order +3 month.
185639	TELINDUS 2401 ADSL ANNEX A S_CTRY3 BU AC/48VDC	Concentrator for 8 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for UK) . 48Vdc and AC power. Manufactured on order +3 month.
182739	TELINDUS 2401 ADSL ANNEX B BU 48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Without internal line splitter option. Redundant 48Vdc. Manufactured on order +3 month.
182740	TELINDUS 2401 ADSL ANNEX B BU AC/ 48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Without internal line splitter option. 48Vdc and AC power. Manufactured on order +3 month.

Sales code	Product name	Description
182574	TELINDUS 2401 ADSL ANNEX B S_CTRY1 BU 48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for standard ISDN 2B1Q). Redundant 48Vdc. Manufactured on order +3 month.
182738	TELINDUS 2401 ADSL ANNEX B S_CTRY1 BU AC/48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for standard ISDN 2B1Q). 48Vdc and AC power. Manufactured on order +3 month.
185640	TELINDUS 2401 ADSL ANNEX B S_CTRY2 BU 48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for ISDN 4B3T & POTS/ ISDN Combi Splitters). Redundant 48Vdc. Manufactured on order +3 month.
185641	TELINDUS 2401 ADSL ANNEX B S_CTRY2 BU AC/48VDC	Concentrator for 8 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links and internal line splitter option included. (suitable for ISDN 4B3T & POTS/ ISDN Combi Splitters). 48Vdc and AC power. Manufactured on order +3 month.
182575	TELINDUS 2402 ADSL ANNEX A BU 48VDC	Concentrator for 16 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. (external line splitter option NOT included) Redundant 48Vdc. Only manufactured on project basis. Manufactured on order +3 month.
182576	TELINDUS 2402 ADSL ANNEX B BU 48VDC	Concentrator for 16 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. (external line splitter option NOT included) Redundant 48Vdc. Only manufactured on project basis. Manufactured on order +3 month.
182577	TELINDUS 2403 ADSL ANNEX A BU 48VDC	Concentrator for 24 ADSL Annex A lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. (external line splitter option NOT included) Redundant 48Vdc. Manufactured on order +3 month.
182578	TELINDUS 2403 ADSL ANNEX B BU 48VDC	Concentrator for 24 ADSL Annex B lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. (external line splitter option NOT included) Redundant 48Vdc. Manufactured on order +3 month.
181305	TELINDUS 2421 SHDSL BU 48VDC	Concentrator for 8 SHDSL lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Redundant 48Vdc. Manufactured on order +3 month.
183065	TELINDUS 2421 SHDSL BU AC/48VDC	Concentrator for 8 SHDSL lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Redundant AC & 48Vdc. Manufactured on order +3 month.
181306	TELINDUS 2422 SHDSL BU 48VDC	Concentrator for 16 SHDSL lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Redundant 48Vdc. Only manufactured on project basis. Manufactured on order +3 month.

Sales code	Product name	Description
181307	TELINDUS 2423 SHDSL BU 48VDC	Concentrator for 24 SHDSL lines and modular uplink interface. ETSI & 19" compliant box. ATM encapsulation on downstream links. Redundant 48Vdc. Manufactured on order +3 month.
184105	TELINDUS 2492 SPLITTER 16P ISDN CTRY1	External ETSI & 19" compliant Splitter box for TELINDUS 2402 ADSL ANNEX B. No PWR required. (suitable for standard ISDN 2BN1Q)Manufactured on order +3 month.
185654	TELINDUS 2492 SPLITTER 16P ISDN CTRY2	External ETSI & 19" compliant Splitter box for TELINDUS 2402 ADSL ANNEX B. No PWR required. (suitable for ISDN 4B3T & POTS/ISDN Combi Splitter). Manufactured on order +3 month.
184104	TELINDUS 2492 SPLITTER 16P POTS CTRY1	External ETSI & 19" compliant Splitter box for TELINDUS 2402 ADSL ANNEX A . No PWR required. (suitable for BEL, NL, IT, Hungary, CHE & FR) . Manufactured on order +3 month.
185650	TELINDUS 2492 SPLITTER 16P POTS CTRY2	External ETSI & 19" compliant Splitter box for TELINDUS 2402 ADSL ANNEX A . No PWR required. (suitable for Poland) . Manufactured on order +3 month.
185651	TELINDUS 2492 SPLITTER 16P POTS CTRY3	External ETSI & 19" compliant Splitter box for TELINDUS 2402 ADSL ANNEX A . No PWR required. (suitable for UK) . Manufactured on order +3 month.
184107	TELINDUS 2493 SPLITTER 24P ISDN CTRY1	External ETSI & 19" compliant Splitter box for TELINDUS 2403 ADSL ANNEX B. (suitable for standard ISDN 2B1Q)Manufactured on order +3 month.
185655	TELINDUS 2493 SPLITTER 24P ISDN CTRY2	External ETSI & 19" compliant Splitter box for TELINDUS 2403 ADSL ANNEX B. (suitable for ISDN 4B3T & POTS/ ISDN Combi Splitter). Manufactured on order +3 month.
184106	TELINDUS 2493 SPLITTER 24P POTS CTRY1	External ETSI & 19" compliant Splitter box for TELINDUS 2403 ADSL ANNEX A. (suitable for BEL, NL, IT, Hungary, CHE & FR). Manufactured on order +3 month.
185652	TELINDUS 2493 SPLITTER 24P POTS CTRY2	External ETSI & 19" compliant Splitter box for TELINDUS 2403 ADSL ANNEX A. (suitable for Poland) . Manufactured on order +3 month.
185653	TELINDUS 2493 SPLITTER 24P POTS CTRY3	External ETSI & 19" compliant Splitter box for TELINDUS 2403 ADSL ANNEX A. (suitable for UK) . Manufactured on order +3 month.
183021	RMK TELINDUS 2400 SERIES	Rack mount kit for MBOX 08 units. Standard included with Telindus 2300 Series, optional for Telindus 2400 Series.
-	TELINDUS 2400 CABLES	To find the sales codes of the cables that can be used on the Telindus 2400 , refer to the Data cables document (PDF) on the Telindus Access Products distribution CD that was delivered with the Telindus 2400.

Index

Symbols

<Struct>, what is 50

<Table>, what is 50

Numerics

4 port Ethernet interface
- alarms 652
- configuration attributes 322
- performance attributes 589
- specifications 705
- status attributes 496

6E1 interface
- alarms 653
- configuration attributes 323
- configuration attributes, general 324
- performance attributes 590
- specifications 705
- status attributes 497
- status attributes, general 498

A

absolute and relative addressing 465

action, what is 51

activating the configuration 112

adding an object to the containment tree 56
- how 58
- in (TMA) CLI 58
- in ATWIN 59
- in the Web Interface 59
- in TMA 58
- referring to the added object 60
- when 57
- which objects 57
- why 57

additional features
- basic configuration 265

address translation
- basic configuration 191
- introducing 192
- NAT, easy NAT 204
- NAT, enabling on an interface 200
- NAT, how works 202
- PAT and NAT, combining 204
- PAT, enabling on an interface 194
- PAT, how works 196
- PAT, limitations and work-around 199
- what is 192
- why use 192

addressing, relative and absolute 465

ADSL Annex, what is 363

ADSL end
- alarms 660
- status attributes 533

ADSL interface
- alarms 655
- alarms, general 656
- configuration attributes 352
- performance attributes 603
- status attributes 515
- status attributes, general 516

ADSL line
- alarms 657
- auto speed 106
- basic configuration 104
- basic configuration attributes 105
- fall-back speed 106
- fixed speed, selecting 106
- performance attributes 604
- specifications 700
- speed (range), selecting 106
- speed range, selecting 106
- speed versus ADSL standard 106
- status attributes 529

ADSL line connector with POTS splitter
- specifications 702

ADSL line pair
- alarms 658
- performance attributes 610
- status attributes 531

ADSL profile
- applying 80
- configuration attributes 362
- creating 75

alarm attributes 641
- configuration 646
- general 648
- introduction 645
- overview 642

alarm configuration attributes 646

alarm in connector specifications 696

alarm in contacts
- alarms 663
- configuration attributes 456

alarm out connector specifications 697

alarms
- 4 port Ethernet interface 652
- 6E1 interface 653
- ADSL end 660
- ADSL interface 655
- ADSL interface, general 656
- ADSL line 657
- ADSL line pair 658
- alarm in contacts 663
- E3/T3 interface 654
- general 649

LAN interface 651
router 662
SHDSL interface 655
SHDSL interface, general 656
SHDSL line 657
SHDSL line pair 658
SHDSL repeater and end 660

application mode, what is 681

application software
downloading 682
in loader mode 687
using FTP 686
using TFTP 684
using TMA 683
using TML 685
version viii
what is 681

ARP cache
how works the 314
proxy ARP 315
time-out 314
what is 314

ATM
basic configuration 116
bridged/routed Ethernet/IP over ATM (RFC 2684), configuring 134
Classical IP (IPoA), configuring 135
introducing 117
IP addresses
automatically obtaining 123
configuring 124
performance attributes 613
PPPoA, configuring 136
PVCs, configuring 126
specifications 707
status attributes 535
UBR, configuring 129
VBR-nrt, configuring 130
what is 117

ATM Adaptation Layers (AAL), what are 118

ATM layers, what are 118

ATM on the E3/T3 interface
basic configuration 159
configuring 161
introducing 160

ATM PVC
bandwidth redistribution 131
configuring 126
what is 117

ATM PVC profile
applying 80
configuration attributes 369
creating 75
using to configure PVCs 126

ATM service categories
traffic parameters 119
what are 119

ATM switching
basic configuration 256
cascading ATM switches 262
configuration attributes 398
configuring 259
introducing 257
performance specifications 709
VC switching, what is 257
VP switching, what is 257
what is 257

attribute
overview 61
what is 50

attribute - action
Activate Configuration 310
clearArpCache 493, 568
clearBridgeCache 568
clearErrorCounter 605
Cold Boot 311
Delete File 575
Load Default Configuration 310
Load Saved Configuration 311
loopbackActivation 528
Rename File 575
resetNat 624
retrain 605
Set Date 485
Set Time 485
startPing 621
stopPing 621
Test Activation (line) 606

attribute - alarm
alarmContactHighMask 647
alarmContactLowMask 647
alarmInfo 648
alarmLevel 646
alarmMask 646
totalAlarmLevel 648

attribute - configuration
accessList 466
adapter 315
addresses 428
addrPools 419
aisDetection 330, 335
alarmFilter 468
alarmLevel
ADSL line object 368
alarm contacts object 457
E1 interface object 330, 336
LAN interface object 319
router object 425
SHDSL line object 361
top object 309
xDSL interface object 353
alarmMask

ADSL line object 368
alarm contacts object 457
E1 interface object 330, 336
LAN interface object 319
router object 425
SHDSL line object 361
top object 309
xDSL interface object 353
algorithm 391
alternativeRoutes 405
arp 314, 447
atmConfig 332
atwinGraphics 469
bootFromFlash 307
bridgeCache 448
bridgeTimeOut 449
bridging 315, 379
cascadeTable 321
cms2Address 465
coding 329
consoleNoTrafficTimeOut 467
countingPolicy 394
crc4Insertion 329
ctrlPortProtocol 462
defaultRoute 402
dhcpCheckAddress 415
dhcpDynamic 413
dhcpStatic 412
dmzHost 429
dns 418
dropLevels 385, 389
dsCorrectionTime 366
dsInterleaveDelay 366
dsMaxSpeed 364
dsMinSpeed 364
espAuthenticationAlgorithm 441
espAuthenticationKey 441
espEncryptionAlgorithm 439
espEncryptionKey 440
filter 444
ftp 467
gateway 428
helperProtocols 409
higherLayerProtocol 372
ifClocking (6E1) 325
ifClocking (DSL) 353
ifClocking (E3/T3) 335
imaDifferentialDelay 327
imaVersion 327
ip 313, 379, 447
ipAddress (loopback) 471
ipNetMask (loopback) 471
ipsecL2tpTunnels 436
l2tpTunnels 431
latency 365
lineConfiguration 353
linkAlarmThresholds 358, 367
localAccess 450
lowdelayQuotum 394
macAddress 451, 455
management 360
masterClock 309
maxFifoQLen 377
maxSpeed 357
maxSpeed2P 357
members 350
method 381
mib2Traps 460
minActiveLinks 350
minSpeed 357
minSpeed2P 357
mode 313, 356, 376
mode (6E1) 325
mode (E3/T3) 335
name 313, 329, 447
oamF5Loopback 377
patAddress 427
portTranslations 427
pppSecretTable 408
priorityPolicy 379
pvc 338, 350, 396
qos 370
queueConfigurations 394
radius 415
region 356
retrain 359, 364
ripHoldDownTime 406
ripUpdateInterval 405
ripv2SecretTable 407
routingProtocol 404
routingTable 403
rxFrameLength 351
security 308
sendAdminUnreachable 411
sendPortUnreachable 411
sendTtlExceeded 410
servicesAvailable 428
snmp 467
spanningTree 449
spi 442
sqThreshold 330, 335
sqTime 330, 335
standard 363
switching 399
sysContact 307
sysLocation 307
sysLog 462
sysName 307
sysSecret 408
tcpSockets 429
tcpSocketTimeOut 429
telnet 467
testDuration 360
tftp 467
timedStatsAvailability 468
timeServer 464
timeZone 464
tos2QueueMapping 387

traceMessages 351
trafficShaping 382
trapDestinations 460
txFrameLength 351
udpSockets 429
udpSocketTimeOut 429
usCorrectionTime 366
usInterleaveDelay 366
usMaxSpeed 364
usMinSpeed 364
vci 370
vlan 316, 451
vlanPriorityMap 389
vlanSwitching 452
vp 348, 350, 397
vpi 370
xdslProfile 396

attribute - performance
addressesAvailable 623
allocFails 623
bridgeAccessList 633
bridgeCache 631
bridgeDiscards 631
bridgeFloods 631
cliSessionCount 635
cms2SessionCount 635
currUsedProcPower 638
d7G703Performance 591, 597
d7G826Performance 592, 598
d7Line 605
d7LineParameters 612
d7Performance 612
discards 623
espAuthenticationFailure 628
espDecryptionFailure 628
espDroppedFrames 628
espSequenceNrReplay 628
freeBlockCount 638
freeDataBuffers 638
freeMemory 639
g703Performance 591, 597
g826Performance 592, 598
h24G703Performance 591, 597
h24G826Performance 592, 598
h24Line 605
h24LineParameters 612
h24Performance 588, 612
h2G703Performance 591, 597
h2G826Performance 592, 598
h2Line 605
h2LineParameters 611
h2Performance 588, 611
icmpAllocs 624
icmpSocketsUsed 623
ifInDiscards 586
ifInErrors 586
ifInNUcastPkts 586
ifInOctets 586
ifInUcastPkts 586
ifInUnknownProtos 586
ifOutDiscards 587
ifOutErrors 587
ifOutNUcastPkts 587
ifOutOctets 587
ifOutQLen 587
ifOutUcastPkts 587
inPackets 628
l2tpTunnels 626
largestFreeBlockSize 638
line 605
lineParameters 612
members 602
outPackets 628
performance 612
pingResults 621
pvc 600, 602, 614
radiusAcct 620
radiusAuth 620
routingTable 619
socketsFree 623
taskInfo 639
tcpAllocs 624
tcPerformance 593
tcpSessionCount 636
tcpSocketsUsed 623
tftpSessionCount 636
totalDataBuffers 638
totalMemory 639
udpAllocs 624
udpSocketsUsed 623
uniStatistics 616
unknownCells 600
usedProcPower 638
vp 600, 616

attribute - status
activeFlash 483
actualBitRate 525
adapter 492
addresses 554
addrPools 552
ais 501, 506
alarmLog 570
arpCache 489, 564
atmSync 508, 536
bootVersion 483
bridgeCache 565
bridging 490, 566
cascadeTable 495
cms2Address 570
configurationSaving 484
corruptBlocks 574
date 485
day 485
deviceId 484, 499, 504
dhcpBinding 550
dhcpRelayInfo 551

dhcpStatistics 550
dns 551
dsInterleaveDelay 532
eocAlarmThresholds 520, 527
eocSoftVersion 527
eocStatus 520, 527
errorCount 521
failure 511
fan 484
feState 510
feTxClockMode 512
fileList 574
flash1Version 482
flash2Version 482
flashVersions 483
freeSpace 574
ifClocking 499
ifDescr 487, 501, 506, 517, 520, 530, 563, 572
ifDsSpeed 530
ifIndex 517
ifLastChange 487
ifModuleClockFreq 484
ifMtu 487, 563, 572
ifOperStatus 487, 501, 506, 517, 520, 524, 530, 563, 572
ifSpeed 487, 501, 506, 520, 524
ifType 487, 501, 506, 517, 520, 530, 563, 572
ifUsSpeed 530
igmpTable 548
ip 488, 563
ipAddress 572
ipAdEntBcastAddr 493
ipAdEntReasmMaxSize 493
ipsecL2tpTunnels 557
l2tpTunnels 556
lfa 501, 506
lineAttenuation 524, 528, 532, 534
loaderVersion 483
los 501, 506
macAddress 488, 563
masterClock 484
members 513
messages 483
neState 510
neTxClockMode 512
noiseMargin 524, 528, 532, 534
numActRxLinks 512
numActTxLinks 512
numDiscoveredRepeaters 520
physLinePair 525
profileUsers 543
progress 532
pvc 508, 510, 536
radius 551
rai 501, 506
region 520
routingTable 546
shdslVersion 527
spanningTree 566
standard 530
stationClockFreq 484
status 524, 532, 574
sysDescr 482
sysObjectID 482
sysServices 482
sysUpTime 482
taskInfo 577
tcCellDeliniation 501
testOriginator 522
testStatus 521
testType 521
time 485
timeServer 570
timeSinceLastRetrain 524, 532
transmitPower 532, 534
usInterleaveDelay 532
vendorId 527, 534
vendorModel 527
vendorRevision 534
vendorSerial 527, 534
vendorSoftVersion 527
vlan 492
vp 508, 541

attribute string, reading vii

auto install 667

B

basic configuration 85
additional features 265
address translation 191
ADSL line 104
ATM 116
ATM on the E3/T3 interface 159
ATM switching 256
bridging 223
DHCP 266
encapsulation on the TIMs 153
encapsulation on the xDSL lines 115
extended access list 271
IMA 154
IP address on the LAN interface 95
IP addresses 87
IPSEC 289
L2TP tunnel 282
passwords 107
policies, traffic and priority
on the bridge 245
on the router 207
policy based routing 176
PPP 137
profiles 63
RIP 182
routing 165
SHDSL line 97
static routing 168

switching 249
VLAN 278
VLAN switching 251

BCP, what is 138

bit string, what is 50

boot mode, what is 680

boot software, what is 680

BootP
how works 668

BootP request, DHCP server reaction on a 414

BootP versus DHCP, releasing IP addresses 414

bridge
configuration attributes 445
performance attributes 629
specifications 709

bridge access list
configuration attributes 454
performance attributes 632

bridge cache
time-out 449
what is 448

bridge group
adding 237
bridge priority, setting 236
bridging protocol, selecting 236
configuration attributes 446
configuring 236
IP address, configuring 236
multiple bridge groups, what are 235
performance attributes 630
status attributes 562
what is 235

bridge port
state transition diagram 229
states 229

bridged/routed Ethernet/IP over ATM (RFC 2684)
configuring 134

bridging
basic configuration 223
bridge group, adding 237
bridge group, configuring 236
bridging attributes, introducing 235
configuring 234
configuring on an interface 240
enabling on an interface 239
explaining the bridging structure 241
introducing 224
versus routing 166
what is 225

bridging structure
explanation 241
where to find 240

C

cascading
configuration attributes 320
status attributes 494

CCP, what is 138

CHAP
authentication in both directions 151
authentication in one direction 150
configuring 149
how works 150
what is 139

child object, what is 50

Classical IP (IPoA), configuring 135

CLP, what is? 122

common TCP and UDP numbers 715

compatibility with other SHDSL devices 103

complex value, what is 50

configuration
activating 112
creating using profiles 74
loading the default 112
using a DIP switch 113

configuration action
executing 110
what is 111

configuration attributes 297
4 port Ethernet interface 322
6E1 interface 323
6E1 interface, general 324
ADSL interface 352
ADSL profile 362
alarm in contacts 456
ATM PVC profile 369
ATM switching 398
bridge 445
bridge access list 454
bridge group 446
cascading 320
default NAT 426
E1 interface, ATM related 331
E1 interface, specific 328
E3/T3 interface 333
E3/T3 interface, ATM related 337
E3/T3 interface, specific 334
forwarding profile 378
general 306
IMA group 349
IPSEC 438
L2TP tunnel 430
LAN interface 312
line configuration profile 395

loopback 470
management 461
manual SA 438
overview 298
priority policy 390
profile 354
router 400
router, general 401
routing filter 443
SHDSL interface 352
SHDSL profile 355
SNMP 459
traffic policy
bridging 388
IP 380

configuration file
creating 673
creating a binary 674
creating an ASCII 675
using CLI get 677
using TFTP get 676
obtaining with TFTP 670

configuration type
active 111
default 111
explanation 111
non-active 111
what is 111

configuring the Telindus 2400 - the concept of profiles 63

connecting
the different parts of the Telindus 2400 27
the Telindus 2400 25
the Telindus 2400, an example 32

connecting with TMA
over an IP network 46
through the control connector 44

containment tree
adding an object 56
of the Telindus 2400 52
terminology 50
what is 50

control connector specifications 694

conventions in this manual
graphical vi
typographical v

copyright notice ii

COS, what is 210

D

default NAT
configuration attributes 426
performance attributes 622
status attributes 553

default route
configuring 170
what is 169

DES and 3DES, what is 291

DHCP
basic configuration 266
dynamic IP addresses, assigning 269
how works 668
introducing 267
relay agent
configuring the Telindus 2400 as 270
what is 267
static IP addresses, assigning 268
what is 267

DHCP server reaction on a BootP request 414

DHCP versus BootP, releasing IP addresses 414

Diff-Serv
AF PHB, what is 209
Diff-Serv, what is 209
PHB, what is 209

dimensions of the Telindus 2400 710

DIP switch table, reading vii

DIP switches 37
DIP switch bank DS1 39
opening and closing the housing 40
overview 39
position on the motherboard 38

directed broadcast, what is 93

DMT, what is 363

DNS, what is 418

document
application software version described in this viii
conventions
graphical vi
typographical v
copyright notice ii
documentation set iv
intended audience viii
organisation iv
properties ii
statements iii
your feedback viii

documentation set iv

downloading
application software 682
in loader mode 687
using FTP 686
using TFTP 684
using TMA 683
using TML 685
files to the file system 690

loader software 688
downloading software 679

E

E1 interface
configuration attributes, ATM related 331
configuration attributes, specific 328
status attributes, specific 500
E1 interface performance definitions 594
E3/T3 interface
alarms 654
configuration attributes 333
configuration attributes, ATM related 337
configuration attributes, specific 334
performance attributes 595
performance attributes, ATM related 599
performance attributes, specific 596
specifications 706
status attributes 502
status attributes, ATM related 507
status attributes, general 503
status attributes, specific 505
easy NAT
example 205
what are the conditions 204
what does 204
what is 204
EFCI, what is 122
element, what is 51
EMC compliance 711
encapsulation on the TIMs
basic configuration 153
encapsulation on the xDSL lines
basic configuration 115
environmental compliance 711
EOC
discovering devices on the SHDSL line 102
how is it handled 102
what is 102
ESP, what is 290
example
ATM on the E3/T3 interface, configuring 162
ATM PVC profile, applying on a line configuration profile 81
ATM PVCs, configuring 127
ATM switches, cascading 263
ATM switching, configuring 261
bridge group, adding multiple 238
custom profile, creating 76
default profile, creating 76
default route, configuring 170
extended access list, configuring 276
forwarding profile, applying on an ATM PVC profile 78
IMA, configuring 158
IP addresses on a PPP link, imposing on the remote 144
IP addresses on an ATM PVC, configuring 124
L2TP tunnel, configuring 287
line configuration profile, applying on an xDSL line 83
NAT, configuring 203
PAT, configuring 195
policy based routing, configuring 180
priority policy on the router, configuring 219
priority policy, applying on an interface 218
priority policy, creating 217
RIP, configuring 185
static route (WAN IP address not present), configuring 173
static route (WAN IP address present), configuring 172
traffic policy on the router, configuring 219
traffic policy, applying on an interface of the bridge 248
traffic policy, applying on an interface of the router 215
traffic policy, creating on the router 214
VLAN switching, configuring 255
xDSL profile, applying on a line configuration profile 81
executing configuration actions 110
extended access list
basic configuration 271
configuring 274
introducing 272
setting up 273
what is 272

F

feedback viii
file system
downloading files 690
status attributes 573
forwarding profile
applying 77
configuration attributes 378
creating 75
Frame Relay
specifications 707
front panels of the Telindus 2400 series 11
front view of the Telindus 2400 26
functional diagram of the Telindus 2400 5

G

general

alarm attributes 648
alarms 649
configuration attributes 306
status attributes 481
group, what is 51

H

HMAC MD5 and SHA-1, what is 291
housing, opening and closing 40

I

ICMP message
communication prohibited 411
port unreachable 411
TTL exceeded 410
ICMP redirect, what is 93
IEEE 802.1P, what is 210
IGMP
topology 548
what is 548
IMA
basic configuration 154
configuring 156
introducing 155
what is 155
IMA group
configuration attributes 349
status attributes 509, 601
what is 155
index name, what is 50
index, what is 50
installation and connection precautions 22
installing and connecting the Telindus 2400 19
installing the Telindus 2400
as rack mount 24
as table top 23
instance name, what is 50
instance value, what is 50
interface
what is 86
introducing
address translation 192
alarm attributes 645
ATM 117
ATM on the E3/T3 interface 160
ATM switching 257
bridging 224
DHCP 267
extended access list 272
IMA 155
IPSEC 290
L2TP tunnel 283
maintenance and management tools 15
management terminology 48
policies, traffic and priority 208
policy based routing 177
PPP 138
RIP 183
routing 166
static routing 169
switching 250
Telindus interface modules (TIMs) 14
the Telindus 2400 3
VLAN 279
VLAN switching 252
IP addresses
automatically obtaining 88
in ATM 123
in PPP 141
on the LAN interface 669
automatically obtaining using BootP or DHCP 668
basic configuration 87
configuring
in ATM 124
in PPP 143
on the LAN interface 95
explaining the IP structure 90
imposing on the remote in PPP 144
private range 192
where to find the IP parameters 89
IP security
performance attributes 627
IP structure
explanation 90
where to find 89
IPCP, what is 138
IPSEC
authentication 291
basic configuration 289
compatibility 291
configuration attributes 438
encapsulation 291
encryption 291
introducing 290
L2TP transport mode, what is 290
modes 290
security association 290
security parameter index 291
security services 290
setting up an IPSEC secured L2TP tunnel 292
what is 290

L

L2TP status
authentication states 561
call states 559

control states 558
delivery states 560

L2TP tunnel
basic configuration 282
configuration attributes 430
encapsulation 284
how works 288
introducing 283
performance attributes 625
setting up 285
status attributes 555
terminology 283
what is 283

LAC, what is 283

LAN interface
alarms 651
configuration attributes 312
performance attributes 585
specifications 703
status attributes 486

LCP, what is 138

LED indicators 33
DCD LED (1 ... 8) 36
introduction 34
power LED (1 / 2) 35
power restart LED (R) 35
SHDSL line LED (DCD) 36
states 34
station clock LED (CLK) 36

line configuration profile
applying 82
configuration attributes 395
creating 79

LNS, what is 283

loader mode, what is 680

loader software
downloading 688
what is 680

loading the default configuration 112
using a DIP switch 113

loopback
configuration attributes 470
status attributes 571

M

maintaining the device 41
with TMA 42

maintenance and management
connection possibilities 17
support 710
tools 15

management
configuration attributes 461
performance attributes 634
status attributes 569

management terminology, introducing 48

manual SA
configuration attributes 438
performance attributes 627

MBS, what is 119

memory, specifications 710

models
how to determine which Telindus 2400 model you have 12
of the Telindus 2400 series 10

motherboard, position of the DIP switches 38

MPoA
what is 121

MS-CHAP
version 1, what is 139
version 2, what is 140

MS-CHAP, what is 139

multi-protocol over ATM
encapsulation mechanisms, which are 121
what is 121

N

NAT
combining with PAT 204
easy NAT 204
enabling on an interface 200
how works 202
what is 192
when use 193

NAT on the LAN interface, a remark 201

O

OAM AIS, what is 615

OAM F4 loop-back cells, what are 122

OAM F5 loop-back cells, what are 122

OAM RDI, what is 615

object, what is 50

operating system
performance attributes 637
status attributes 576

organisation of this manual iv

overview
alarm attributes 642
configuration attributes 298
performance attributes 580
status attributes 474

overview of the Telindus 2400 series 9

over-voltage and over-current protection compliance 711

P

PAP
- authentication in both directions 148
- authentication in one direction 147
- configuring 146
- how works 147
- what is 139

parent object, what is 50

parts of the Telindus 2400 27

passwords
- adding to the security table 108
- basic configuration 107
- correcting the security table 108
- entering in the different management tools 109
- remarks on 308

PAT
- combining with NAT 204
- enabling on an interface 194
- how works 196
- limitations and work-around 199
- what is 192
- when use 193

PCR, what is 119

performance attributes 579
- 4 port Ethernet interface 589
- 6E1 interface 590
- ADSL interface 603
- ADSL line 604
- ADSL line pair 610
- ATM 613
- bridge 629
- bridge access list 632
- bridge group 630
- default NAT 622
- E1 interface performance definitions 594
- E3/T3 interface 595
- E3/T3 interface, ATM related 599
- E3/T3 interface, specific 596
- IP security 627
- L2TP tunnel 625
- LAN interface 585
- management 634
- manual SA 627
- operating system 637
- overview 580
- router 617
- router, general 618
- SHDSL interface 603
- SHDSL line 604
- SHDSL line pair 610

policies, traffic and priority
- configuring on the bridge 246
- configuring on the router 212
- introducing 208
- on routed and on bridged data 211
- on the bridge
  - basic configuration 245
- on the router
  - basic configuration 207

policy based routing
- basic configuration 176
- introducing 177
- setting up 178
- what is 177

power requirements 693

PPP
- basic configuration 137
- CHAP, configuring 149
- CHAP, how works 150
- handshake 138
- introducing 138
- IP addresses
  - automatically obtaining 141
  - configuring 143
  - imposing on the remote 144
- link monitoring, configuring 145
- PAP, configuring 146
- PAP, how works 147
- specifications 707
- what is 138

PPP link monitoring
- configuring 145
- what is 138

PPPoA
- configuring 136
- what is 122

priority policy
- applying on an interface 218
- configuration attributes 390
- creating 216
- what is 208

priority queuing, what is 208

product information 717

profile
- ADSL profile, applying 80
- ADSL profile, creating 75
- ATM PVC profile, applying 80
- ATM PVC profile, creating 75
- basic configuration 63
- configuration attributes 354
- creating a configuration using 74
- custom, what is 68
- default, what is 68
- explaining 64
- forwarding profile, applying 77
- forwarding profile, creating 75
- line configuration profile, applying 82

line configuration profile, creating 79
linking the different profiles together 70
linking the different profiles together, an example 73
SHDSL profile, applying 80
SHDSL profile, creating 75
status attributes 542
what is 65
which are there 66

profile objects, short description
bridging_default and bridging 71
bridgingTrafficPolicy 71
interface(dsl_x) 72
ipTrafficPolicy 71
priorityPolicy 71
pvc_default and pvc 72
routing_default and routing 71
xdsl_default and xdsl 72
xdslAtm_default and xdslAtm 72

proxy ARP, what is 315

R

RADIUS
what is 418

reading
a DIP switch table vii
an attribute string vii

referring to an added object
example 60
how to 60
what is 60

relative and absolute addressing 465

relay agent for BootP and DHCP requests 668

releasing IP addresses, DHCP versus BootP 414

remarks on
ATM idle cell format 332
bridging traffic policy on the LAN interface 248
compression attribute 347, 375
creating a dual pair line 100
dhcpStatistics attribute 550
extended access list using the trafficShaping table 274
gatewayPreference in PPP on the xDSL lines versus the 6E1 interface 143
helperProtocols attribute 409
ifClocking = masterClock 325, 335
ifOperStatus of the WAN interface 518
IP address on the LAN interface in case of bridging 89, 167, 239, 313, 447
ipIntervalPool attribute 423
ipListPool attribute 420
l2tpTunnels configuration attribute 286, 432
latency attribute 365
loopbackActivation action 528
masterClock = ifModule 309
messages attribute 483
natAddresses attribute 201
passwords 308
PPP authentication on the xDSL lines versus the 6E1 interface 146, 149
rerouting principle 175
resetNat action 624
rip2Authentication attribute 189
ripv2SecretTable attribute 407
routing traffic policy on the LAN interface 93, 215
routing update filter 444
selecting a speed range on the 2 pair version 99
standard attribute (ADSL profile) 363
telnet attribute 467
testActivation 606
trafficShaping 382
VLANs on the LAN and VLAN switching 252, 279
vlanSwitching attribute 254, 453

rerouting principle, what is 175

RIP
authentication, enabling on an interface 190
basic configuration 182
enabling on an interface 184
explaining the RIP structure 186
how works 183
introducing 183
support 183
what is 183

RIP authentication
enabling on an interface 190
what is 183

RIP hold-down timer, what is 406

RIP structure, explanation 186

router
alarms 662
configuration attributes 400
configuration attributes, general 401
performance attributes 617
performance attributes, general 618
specifications 709
status attributes 544
status attributes, general 545

routing
basic activities 166
basic configuration 165
determining the optimal path 166
enabling on an interface 167
introducing 166
static versus dynamic 169
transporting packets 166
versus bridging 166

what is 166
routing and bridging performance specifications 709
routing filter
configuration attributes 443
routing table
configuring 171
rules of thumb when configuring 174
what is 169

S

SA, what is 290
safety
compliance 711
instructions 20
requirements ii
sales codes 717
SCR, what is 119
security table
adding passwords 108
correcting 108
self-learning bridge, what is 226
setting up an xDSL connection 63
SHDSL interface
alarms 655
alarms, general 656
configuration attributes 352
performance attributes 603
status attributes 515
status attributes, general 516
SHDSL line
alarms 657
auto speed 99
basic configuration 97
basic configuration attributes 98
channel attribute (fixed to central) 101
compatibility with other SHDSL devices 103
dual pair line, creating 100
eocHandling attribute (fixed to alarmConfiguration) 102
fall-back speed 99
fixed attributes 101
fixed speed, selecting 99
performance attributes 604
power back-off, what is 101
retrain criteria 359
specifications 699
maximum covered distance 699
speed (range), selecting 99
speed range, selecting 99
status attributes 519
timingMode attribute (fixed to synchronous) 101
SHDSL line pair
alarms 658
performance attributes 610
status attributes 523
SHDSL profile
applying 80
configuration attributes 355
creating 75
SHDSL repeater and end
alarms 660
status attributes 526
simplified protocol diagram of the Telindus 2400 6
SNMP
configuration attributes 459
SNTP, what is 464
software
downloading 679
what is boot, loader and application 680
Spanning Tree
behaviour 231
bridge failure 231
bridging loops 231
network extension 231
BPDU 230
propagation of 230
what is 230
bridge port states 229
bridge priority, what is 232
path cost, what is 232
port priority, what is 232
priority and cost 232
root bridge 227
how selected 227
what is 227
topology 228
specifications
2400 models 692
4 port Ethernet interface 705
6E1 interface 705
ADSL line 700
ADSL line connector with POTS splitter 702
alarm in connector 696
alarm out connector 697
ATM encapsulation 707
ATM switching performance 709
bridging 709
control connector 694
dimensions 710
E3/T3 interface 706
EMC compliance 711
environmental compliance 711
Frame Relay encapsulation 707
LAN interface 703
maintenance and management support 710

memory 710
over-voltage and over-current protection compliance 711
power requirements 693
PPP encapsulation 707
routing 709
routing and bridging performance 709
safety compliance 711
SHDSL line 699
maximum covered distance 699
station clock connector 695
TIM interface 704
xDSL line 698
xDSL line connector 701

SPI, what is 291

statements iii

static routing
basic configuration 168
default route, configuring 170
introducing 169
routing table, configuring 171

station clock connector specifications 695

status attributes 473
4 port Ethernet interface 496
6E1 interface 497
6E1 interface, general 498
ADSL end 533
ADSL interface 515
ADSL interface, general 516
ADSL line 529
ADSL line pair 531
ATM 535
bridge group 562
cascading 494
default NAT 553
E1 interface, specific 500
E3/T3 interface 502
E3/T3 interface, ATM related 507
E3/T3 interface, general 503
E3/T3 interface, specific 505
file system 573
general 481
IMA group 509, 601
L2TP tunnel 555
LAN interface 486
loopback 571
management 569
operating system 576
overview 474
profile 542
router 544
router, general 545
SHDSL interface 515
SHDSL interface, general 516
SHDSL line 519
SHDSL line pair 523
SHDSL repeater and end 526

structured value, what is 50

switching
available switches 250
basic configuration 249
introducing 250
what is 250

syslog, what is 463

T

technical specifications 691

Telindus 2400
functional diagram 5
how to determine which model you have 12
introducing 3
series overview 9
simplified protocol diagram 6
the different front panels 11
the different models 10
what is 4

Telindus interface modules (TIMs)
inserting in the Telindus 2400 31
introducing 14
overview 14

TIM interface
specifications 704

Time To Live (TTL), what is 410

TMA
connecting over an IP network 46
connecting through the control connector 44
how to connect 43
maintaining the device with 42
what is 43

TMA sub-system picture 665
how to display 665
structure 665

TOS
AF PHB, what is 209
DSCP, what is 209
PHB, what is 209
precedence field, what is 209
TOS byte, what is 209
TOS field, what is 209

traffic policy
applying on an interface of the bridge 248
applying on an interface of the router 215
configuration attributes of the bridge 388
configuration attributes of the router 380
configuring an extended access list 271
creating on the bridge 247
creating on the router 213
what is 208

Transparent Spanning Tree bridge, what is 226

troubleshooting the Telindus 2400 114

U

UBR
configuring 129
what is 120

unpacking 21

UTC, what is 464

V

value, what is 50

VBR-nrt
configuring 130
what is 120

VC switching, what is 257

VCI, what is 117

VLAN
basic configuration 278
creating 280
introducing 279
local or global tag significance 319
what is 279

VLAN switching
basic configuration 251
configuring 253
introducing 252
stripping the VLAN tag 452
what is 252

VLAN tag, what is 279

VP switching, what is 257

VPI, what is 117

W

warning
EMC 22
ESD 22
important safety instructions 20
safety 20

X

xDSL connection, setting up 63

xDSL line
specifications 698

xDSL line connector
specifications 701